Fachhochschule Köln
Cologne University of Applied Sciences

Authentizität und Integrität von Teilnehmerdaten in sozialen Netzwerken ohne zentrale Organisationseinheit

Authenticity and integrity of participant data in social networks without a central authority

Masterthesis

ausgearbeitet von

Benjamin Krumnow

zur Erlangung des akademischen Grades

Master of Science

vorgelegt an der
Fachhochschule Köln
Campus Gummersbach
Fakultät für Informatik und
Ingenieurwissenschaften

im Studiengang

Medieninformatik

Erster Prüfer: Prof. Dr. Kristian Fischer
Fachhochschule Köln

Zweiter Prüfer: Prof. Dr. Stefan Karsch
Fachhochschule Köln

Gummersbach, im Dezember 2013

Adressen: Benjamin Krumnow
Eschenbachstr. 9
50739 Köln
Benjamin.Krumnow@googlemail.com

Prof. Dr. Kristian Fischer
Fachhochschule Köln
Institut für Informatik
Steinmüllerallee 1
51643 Gummersbach
Fischer@fh-koeln.de

Prof. Dr. Stefan Karsch
Fachhochschule Köln
Institut für Informatik
Steinmüllerallee 1
51643 Gummersbach
Karsch@gm.fh-koeln.de

Kurzfassung

Soziale Netzwerke decken ein breites Spektrum an Anwendungsfällen ab und bieten somit eine Vielzahl an Funktionen, bei denen die Teilnehmer mit ihrem sozialen Umfeld interagieren und mit anderen Informationen teilen können. Die dabei aufkommenden Informationen über die Teilnehmer müssen teilweise erfasst und gespeichert werden, um die Funktionalität und die Gebrauchstauglichkeit des sozialen Netzwerkes zu sichern und Missbrauch vorzubeugen. Dies jedoch hat den Nachteil, dass die entstandenen Daten und somit eine Reihe von Aktivitäten der Teilnehmer durch den Anbieter eines sozialen Netzwerkes beobachtet werden können. Um die Privatsphäre der Teilnehmer zu schützen oder auch um eine bessere Skalierbarkeit der sozialen Netzwerke zu erreichen, konzentrieren sich aktuelle Forschungsarbeiten auf die Dezentralisierung sozialer Netzwerke. Dies führt zu neuen Herausforderungen, da die Aufgaben der zentralen Organisationseinheit auf mehrere Komponenten verteilt werden müssen. Eine dieser Aufgaben ist es, die Authentizität und Integrität der Daten für die Teilnehmer sicher zustellen. Die Vernachlässigung dieser beiden Schutzziele kann zu Missbrauch und verschiedenen Angriffen auf ein soziales Netzwerk und dessen Teilnehmer führen.

Um an diese Problemstellung heranzugehen, soll innerhalb dieser Arbeit geklärt werden, wann und welche Mechanismen für die Erfüllung der beiden Schutzziele in sozialen Netzwerken ohne zentrale Organisationseinheit geeignet sind. Hierfür werden die Angriffe zur Verletzung dieser beiden Schutzziele in soziale Netzwerken und der darunter liegenden Infrastruktur betrachtet. Des Weiteren wird geklärt, welchen Einfluss die Dezentralisierung auf die die Teilnehmerdaten hat und was die relevanten Kriterien für authentische Teilnehmerdaten sind.

Abstract

Social networks cover a wide range of use cases and thus offer a variety of functions in which the participants can interact with their social environment and share information. In this process, the emerging information about the participants must be partially captured and stored to ensure the functionality, usability and to prevent abuse. The disadvantage is that the resulting data and thus a number of activities of the participants can be observed by the provider of a social network. To protect the participants' privacy or to achieve better scalability of social networks, actual research focuses on the decentralization of social networks. This leads to new challenges because the responsibilities of the central organization must be distributed over several components. One of these challenges is to provide the authenticity and integrity of the data for the participants. The neglect of these two security objectives can lead to abuse and various attacks on a social network and its participants.

To approach this problem the goal is to resolve when and which kind of mechanisms satsify the two security objectives in social networks without a central organization. Therefore the attacks for violating these security objectives in social networks and the underlying infrastructure are considered. In addition to that it will be clarified what the impact of decentralization on participant data is and what the relevant criteria for authentic participant data are.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ABE	Attribute-based Encryption
API	Application Programming Interface
DDM	Distributed Data Mining
DDoS	Distributed-Denial-of-Service
DHT	Distributed Hash Table
DNS	Domain Name System
DoS	Denial-of-Service
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol Secure
ISP	Internet Service Provider
MANET	Mobile Ad-hoc Network
P2P	Peer-to-Peer
PKI	Public-Key-Infrastruktur
PPDDM	Privacy-Preserving Distributed Data Mining
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VIS	Virtual Individual Server

1 Einführung

Das Internet, in dem ein großer Teil unserer Kommunikation stattfindet, ist mittlerweile ein fester Bestandteil der heutigen Gesellschaft. Innerhalb dieses Mediums tauschen die Nutzer Information aus, kommunizieren miteinander oder pflegen soziale Beziehungen. Um dies zu ermöglichen existiert eine Vielzahl an technischen Lösungen, wobei eine der populärsten soziale Netzwerke sind. Diese ermöglichen es den Nutzern eigene Profile zu erstellen und Verbindungen mit anderen Nutzern einzugehen. Darüber hinaus bieten sie ein umfangreiches Repertoire von Funktionen und eine geringe Einstiegshürde, da die Nutzer meist nicht mehr als einen Webbrowser und einen Account benötigen, um an dem sozialen Netzwerk teilzunehmen.

Bei den erfolgreichsten sozialen Netzwerken handelt es sich um Dienste im Web, die von einem zentralen Dienstanbieter betrieben werden und dadurch auch eine Reihe an Problemen mit sich bringen. Eines dieser Probleme ist, dass die Infrastruktur, um den Dienst zu betreiben, von einem Anbieter gestellt wird. Daraus resultiert eine geringe Skalierbarkeit, denn umso mehr Benutzer die Plattform nutzen, desto mehr Last entsteht auf den Servern des Betreibers, was wiederum zu höheren Kosten, durch den steigenden Rechen- und Energiebedarf, führt. Zusätzlich kann dies ein zentraler Schwachpunkt der Verfügbarkeit sein, denn bei einem Ausfall der Infrastruktur des Dienstanbieters ist das komplette Netzwerk betroffen. Ein anderes Problem ist die stets präsente Gefahr der Verletzung der Privatsphäre der Nutzer, denn soziale Netzwerke speichern eine Vielzahl an Daten der Teilnehmer. Dies kann zum einen notwendig sein, um die grundlegende Funktionalität oder die Gebrauchstauglichkeit der Plattformen zu gewährleisten. Zum anderen bietet dies aber auch die Möglichkeit für Data Mining, wodurch sich Informationen über die Nutzer beziehen lassen, welche über die Daten, die der Nutzer über sich bewusst preisgibt, hinaus gehen. Zudem kann in einem zentral organisierten sozialen Netzwerk jeder Schritt eines Benutzers von dem Dienstanbieter beobachtet werden, da alle Aktionen, die der Nutzer tätigt, über die Systeme eines Anbieters gehen. Bei den Dienstanbietern selbst handelt es sich meist um profitorientierte Unternehmen, die diese Daten zur Monetarisierung durch das Einblenden von Werbung, welche auf die Präferenzen und Eigenschaften der Nutzer abgestimmt sind, verwenden. Zusätzlich haben meist auch Drittanbieter, die Applikationen innerhalb eines sozialen Netzwerkes anbieten, Zugriff auf die Daten der Teilnehmer [19].

Um diesen Problemen entgegenzuwirken, setzen aktuelle Ansätze und Forschungen auf die Dezentralisierung von sozialen Netzwerken. Hierbei wird die Last auf

mehrere unabhängige Anbieter bzw. Teilnehmer verteilt, wobei zusätzlich eine höhere Verfügbarkeit erreicht werden kann, da auch bei Ausfällen eines oder mehrerer Anbieter bzw. Teilnehmer die Funktionsfähigkeit des Netzes erhalten bleibt. Des Weiteren obliegen die Teilnehmerdaten nicht mehr einem Anbieter und können mit entsprechender Verschlüsselung gegen Zugriffe gesichert werden. Ebenso wird die Überwachung der Teilnehmer erschwert, wenn die Aktionen der Teilnehmer über verschiedene Instanzen getätigt werden. Hinzu kommen weitere Vorteile, die durch die Dezentralisierung entstehen, wie ein erhöhter Schutz vor Zensur, da Teilnehmerdaten nur bedingt durch eine Organisationseinheit manipuliert werden können oder dass das soziale Netzwerk unabhängig von der allgemeinen Kommunikationsinfrastruktur genutzt werden kann. So können die Nutzer der sozialen Netzwerke auf mobile Ad-hoc Netzwerke (MANETs) ausweichen, wenn in Krisensituationen die Kommunikationsinfrastruktur ausfällt [6, 38, 72].

Die Dezentralisierung dieser Dienste bringt allerdings auch neue Herausforderungen mit sich, welche die Sicherheit, das Verteilen von Informationen, den Umgang mit heterogenen Plattformen und die Datenhaltung in diesen Netzwerken betreffen. Dies wirkt sich unter anderem auf die Teilnehmerdaten aus, welche nicht nur für die grundlegenden Funktionen wichtig sind, sondern auch den Teilnehmern beispielsweise helfen andere Teilnehmer zu finden oder zu entscheiden, ob diese glaubwürdig [49, 64] sind. Des Weiteren lassen sich die Teilnehmerdaten zum automatisierten Erkennen von Spam [7, 59] oder von Fehlinformationen [15, 34, 43] verwenden. Allerdings führt die Dezentralisierung von sozialen Netzwerken auch dazu, dass eine zentrale Organisationseinheit in dem Netzwerk nicht mehr existiert oder nur noch bedingt die Daten der Teilnehmer protokollieren kann. Dadurch entstehen neue Möglichkeiten, um Angriffe auf die Integrität und Authentizität der Teilnehmerdaten durchzuführen. Diese beiden Schutzziele für Teilnehmerdaten in sozialen Netzwerken ohne eine zentrale Organisationseinheit zu wahren, stellt eine Herausforderung innerhalb dieses zukunftsweisenden Themengebietes dar.

1.1 Motivation zur Verwendung von Teilnehmerdaten

Da die Privatsphäre eine der grundlegenden Anreize für die Entwicklung und Nutzung eines sozialen Netzwerkes ohne eine zentrale Organisationseinheit ist, können hierbei gegensätzliche Interessen zu dem Sammeln und Speichern von Teilnehmerdaten existieren. Denn liegen diese Daten erst einmal bei einer anderen Instanz vor, besteht die Möglichkeit, dass diese an Dritte weiter gegeben werden. Ebenso stellt

die Existenz der Daten ein potentielles Risiko dar, dass unbefugte Personen sich möglicherweise Zugriff zu diesen Daten verschaffen. Ein Ansatz um diesem Risiko zu begegnen, ist die Verwendung von kryptographischen Verfahren in den sozialen Netzwerken ohne zentrale Organisationseinheiten. Trotzdem bleibt die Gefahr, dass ein Teilnehmer die Daten weitergibt oder ein Angreifer versucht die Daten zu erheben und diese Informationen gegen den Teilnehmer oder andere Personen zu verwenden. Für die Teilnehmer kann es also ein Anreiz sein, möglichst keine, falsche oder nur die notwendigen Daten von sich preiszugeben. Ebenso können soziale Netzwerke, die auf Schutz der Privatsphäre oder Anonymität ausgelegt sind, versuchen möglichst viele Daten der Teilnehmer zu verschleiern oder nicht zu erheben. Allerdings gibt es Anwendungsfälle, in denen authentische Daten und der Verzicht auf vollständige Anonymität ihre Relevanz haben. Dabei muss beachtet werden, dass soziale Netzwerke von der Definition[1] her, durch die Erstellung eines personenbezogenen Profils und dem Eingehen von Verbindungen mit anderen Teilnehmern, darauf ausgelegt sind, dass die Teilnehmer Information über sich für andere preisgeben. Somit besteht das soziale Netzwerk aus Informationen, die die Teilnehmer in das Netzwerk geben. Dazu kommt, dass unterschiedliche Motivationen für einen Teilnehmer existieren, um Informationen über sich preiszugeben. Eine Motivation kann hierbei sein Erfahrungen und Erlebnisse mit anderen Menschen teilen zu wollen oder aus dem Erfordernis entstehen, dass Teilnehmer zum Eingehen von sozialen Beziehungen andere Teilnehmer anhand von Merkmalen identifizieren müssen. Das Suchen von anderen Teilnehmern erfordert authentische Teilnehmerdaten, mit denen ein Profil zu einer realen Identität zugeordnet werden kann, wenn vorher keine eindeutigen Kontaktmöglichkeiten gegeben wurden, wie etwa ein Pseudonym. Dabei ist es in einigen Fällen nicht ausreichend, den Namen eines Benutzers zu kennen, wenn gleiche Namensbezeichnungen in dem Netzwerk möglich sind. Hierfür können weitere Kriterien herangezogen werden, wie beispielsweise das Alter, der Wohnort, das Profilbild, der Beruf oder die sozialen Beziehungen. Ein weiterer Aspekt, bei dem authentische Teilnehmerdaten helfen können, ist das Aufbauen von Vertrauen zwischen den Teilnehmern. Beispielsweise kann eine Person die Vertrauenswürdigkeit eines anderen Teilnehmers bestimmen, wenn beide eine hohe Schnittmenge an sozialen Beziehungen haben oder die Beiträge, die über den jeweiligen Account verfasst werden, authentisch im Hinblick auf die Person wirken. Gibt ein Teilnehmer diese Daten allerdings öffentlich frei, so können diese Informationen auch von Personen ohne eine direkte Verbindung zu dem Teilnehmer eingesehen und verwendet werden. Eine andere Möglichkeit zum Gewinnen

[1] Siehe hierzu die Definition aus 2.1.

von Vertrauen kann das Beobachten der Aussagen und Handlungen der Teilnehmer des sozialen Netzwerkes gegenüber eines anderen Teilnehmers sein. Bekommt beispielsweise ein Teilnehmer Zustimmung in dem Netzwerk, kann dies ein Indikator für Kompetenzen, Authentizität oder andere Eigenschaften des Teilnehmer sein. Auf der Gegenseite kann bei dem Fehlen von authentischen Teilnehmerdaten das Bilden von Vertrauen, Unterscheiden oder Finden von anderen Teilnehmern erschwert sein. Des Weiteren kann dies die Grundlage eines Angriffes bilden oder zum Missbrauch verhelfen.

Zu diesen Aspekten ermöglicht die Ansammlung von Teilnehmerdaten das Auswerten und die Informationsgewinnung durch Data Mining. Data Mining kann zum einen durch die jeweilige Organisationseinheit betrieben werden, ohne dass die Teilnehmer dies unterbinden können. Zum anderen können auch andere Institutionen oder Unternehmen Data Mining betreiben, wenn die Daten frei zugänglich sind oder eine Organisationseinheit die Daten für ein Unternehmen zur Verfügung stellt. Eine grundlegenden Motivation der Dienstanbieter dabei ist es, Informationen für das Marketing zu gewinnen. Dies wirft jedoch einige Fragen zur Privatsphäre auf, da es hierdurch möglich ist, neue Informationen über die Teilnehmer zu erhalten, die die Teilnehmer selber möglicherweise nicht preisgeben möchten. Die neu gewonnenen Informationen können unter anderem sensible Informationen aufdecken, wie beispielsweise die sexuelle Orientierung eines Teilnehmers.[2] Auf der anderen Seite lässt sich Data Mining auch für positive Aspekte, wie die Sicherung von Informationsqualität oder zur Umsetzung von erweiterten Funktionen für die Teilnehmer einsetzen. Dazu gehören beispielsweise das automatische Erkennen von Spam bzw. Spammern, das Eingrenzen der Verbreitung von Gerüchten oder die Verbesserung bzw. Anpassung des sozialen Netzwerkes durch das Auswerten des Verhaltens der Teilnehmer.

Die in diesem Abschnitt angesprochenen Punkte und Beispiele stellen einen Ausschnitt von Anwendungsfällen dar, die die gegensätzlichen Interessen, zwischen dem Nutzen aus Teilnehmerdaten und dem Schutz der Privatsphäre, verdeutlichen sollen. Diesen Interessen beiderseitig zufriedenstellend nachzukommen, ist meist nur schwer oder gar nicht möglich. Können diese nicht gleichzeitig erfüllt werden, führt dies zu Kompromissen oder einer Priorisierung von Interessen, welche es je nach Situation abzuwägen gilt. In einem sozialen Netzwerk, in dem ein Teilnehmer mit einem kleinen Kreis von sich nahestehenden Personen kommunizieren möchte, hat

[2] siehe hierzu http://firstmonday.org/ojs/index.php/fm/article/view/2611/2302, letzte Sichtung am 07.11.2013

die Privatsphäre möglicherweise eine höhere Priorität als in einem Netzwerk, in dem sich die Teilnehmer öffentlich präsentieren und mit fremden Personen in Kontakt treten. Des Weiteren können die Umstände die Priorisierung entsprechend beeinflussen. Teilnehmer in einem sozialen Netzwerk, in dem viel Missbrauch betrieben wird, wie durch eine Flut von Spam oder Fehlinformationen, sind möglicherweise eher dazu motiviert, einer Auswertung von Teilnehmerdaten zuzustimmen, um dafür eine bessere Gebrauchstauglichkeit und Informationsqualität zu erreichen.

1.2 Zielsetzung

Für die Entwicklung eines dezentralen sozialen Netzwerkes müssen eine Reihe an Designentscheidungen getroffen werden, um die Funktionen, welche über eine zentrale Organisationseinheit realisiert sind, in einer dezentralen Umgebung zu ermöglichen. Hierbei sind mittlerweile verschiedene Ausprägungen von sozialen Netzwerken entstanden, die den Schutz der Privatsphäre oder eine bessere Skalierbarkeit beabsichtigen. Innerhalb dieser Ausprägungen kommen auch verschiedene Konzepte zur Umsetzung der Schutzziele Integrität und Authentizität zum Einsatz. Durch die Dezentralisierung von sozialen Netzwerken existiert keine vertrauenswürdige Instanz in Form einer zentralen Organisationseinheit, welche über die Daten verfügt und die Integrität sowie Authentizität dieser Daten für die Teilnehmer gewährleistet. Um allerdings die Vorteile, der oben angemerkten Verfahren zu nutzen, werden authentische und integere Teilnehmerdaten als Grundlage benötigt. Aus diesem Grund ist das Ziel dieser Masterthesis Mechanismen, welche zum Schutz der Integrität und Authentizität von Teilnehmerdaten in sozialen Netzwerken ohne eine zentrale Organisationeinheit beitragen können, zu identifizieren und zu bewerten. Da allerdings eine der grundlegenden Motivationen zum Entwerfen und Nutzen eines sozialen Netzwerkes ohne eine zentrale Organisationseinheit, die Privatsphäre ist, gilt auch diesen Aspekt sowie weitere einschneidende Auswirkungen der Maßnahmen bei einer Bewertung zu berücksichtigen. Um geeignete Maßnahmen zu ermitteln, werden zum einen die möglichen Angriffe betrachtet und zum anderen Teilnehmerdaten in sozialen Netzwerken analysiert. Hierfür wird betrachtet, wie die Authentizität dieser Daten im einzelnen bestimmt ist. Des Weiteren wird zum Identifizieren von Bereichen, in denen entsprechende Mechanismen ansetzen müssen, der Umgang mit Teilnehmerdaten in den verschiedenen Dezentralisierungsformen betrachtet.

1.3 Überblick

Diese Arbeit umfasst sieben Kapitel, wobei sich Kapitel 2 mit der Definition von sozialen Netzwerken und wie sich diese kategorisieren lassen, beschäftigt. Des Weiteren werden die Bedeutung der Schutzziele aus der IT-Sicherheit und die Konzepte von Vertrauen, Reputation und Glaubwürdigkeit erläutert, um ein Verständnis für die grundlegenden Begriffe der Domäne für diese Arbeit zu schaffen. Danach werden in Kapitel 3 die Ausgangssituation und die Angriffe für soziale Netzwerke ohne eine zentrale Organisationseinheit beschrieben, um mögliche Bereiche für Abwehrmechanismen zu identifizieren. Die verschiedenen Ausprägungen von Teilnehmerdaten werden in Kapitel 4 erfasst. Hierfür werden unter anderem Verfahren für die Glaubwürdigkeitsbestimmung, Verhaltensanalyse und Spamerkennung vorgestellt. Mit diesen Ergebnissen wird eine eigene Klassifikation für Teilnehmerdaten entwickelt. Die Auswirkungen der Dezentralisierung auf die Teilnehmerdaten werden danach in Kapitel 5 vorgestellt. Dabei wird erläutert, welche Formen der Dezentralisierung von sozialen Netzwerken es gibt, welche Sicherheitsmechanismen verwendet werden und welchen Einfluss diese beiden Faktoren auf die einzelnen Kategorien der Teilnehmerdaten haben. In Kapitel 6 erfolgt dann die Betrachtung und Bewertung der Maßnahmen, um eventuell verloren gegangene Informationen wieder für die oben genannten Verfahren verfügbar zu machen und dabei die Schutzziele zu erfüllen. Im Anschluss daran werden in Kapitel 7 die Erkenntnisse aus dieser Arbeit zusammengefasst und ein Ausblick auf mögliche zukünftige Arbeiten gegeben.

2 Grundlagen

Dieses Kapitel wird dafür genutzt, die grundlegenden Begriffe der Domäne und eine Einführung in soziale Netzwerke zu geben. Hierfür wird in den Abschnitten 2.1 bis 2.3 auf den Begriff soziales Netzwerk und dessen Bedeutung für diese Arbeit eingegangen. Des Weiteren werden verschiedene Ausprägungen von sozialen Netzwerken und einige grundlegende Funktionen von zwei der bekanntesten Plattformen, Twitter[3] und Facebook[4], vorgestellt. Danach werden die Schutzziele aus der IT-Sicherheit behandelt und welche Rolle sie in dieser Arbeit einnehmen. Die daran anschließenden Abschnitte beschäftigen sich unter anderem mit der Bedeutung von Vertrauen, Reputation und Glaubwürdigkeit, da diese für das Verständnis der behandelten Verfahren aus Kapitel 4, 5 und 6 eine wichtige Basis darstellen.

2.1 Soziale Netzwerke

Der Begriff *soziales Netzwerke* stammt aus der Soziologie und bezeichnet nach Wasserman und Faust [63, S. 9] eine begrenzte Menge von Personen und die Beziehungen zwischen ihnen. Oft werden mit diesem Begriff auch Online-Plattformen wie Facebook, Xing und Twitter assoziiert, welche allerdings in englischsprachigen, wissenschaftlichen Publikationen unter den Begriffen Social Network Site, Social Network Service, Online Social Network und Web-based Social Networks geführt werden. Ebenso, wie eine Vielfalt von Begriffen für soziale Netzwerke, gibt es zu auch mehrere Definitionen. Ellison und Boyd definieren soziale Online-Netzwerke über die Funktionalität, die die Dienste anbieten:

> „*[...] as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.*" [12, S. 211]

Diese Definition wird von Cutillo et al. [19] sowie Datta et al. [21] aufgegriffen und um zusätzliche Funktionen ergänzt beziehungsweise modifiziert. Die Änderungen umfassen, dass ein Nutzer mit anderen Nutzern oder der Öffentlichkeit Inhalte teilen kann und dass die Plattform das Erstellen und Benutzen von Drittanbieteranwendungen unterstützt.

[3] https://twitter.com/about, letzte Sichtung 30.11.2013
[4] www.facebook.com, letzte Sichtung 30.11.2013

In der Definition von Golbeck [31] für eine Studie wird dagegen eine stärkere Einschränkung von möglichen Plattformen vorgenommen. Damit eine Plattform als soziales Online-Netzwerk gilt, muss sie über einen Webbrowser erreichbar sein, den Teilnehmern eine Funktion anbieten, ihre Beziehung zu anderen Teilnehmern zu definieren. Diese Beziehungen zu anderen Nutzern müssen explizit angeben werden und dürfen nicht das Ergebnis einer anderen Interaktion sein. Des Weiteren muss die Plattform es ermöglich Beziehungen einzusehen und zu durchsuchen. Die Eigenschaft, dass ein soziales Online-Netzwerk über einen Webbrowser abrufbar sein muss, schließt soziale Netzwerke aus, die zur Nutzung zusätzliche Software auf dem Client benötigen, damit ein Nutzer an dem Netzwerk teilnehmen kann. Dies kann auch zum Ausschluss von Chat- und Videochat-Plattformen führen, die beispielsweise meist die ersten zwei Funktionen von der Definition von Ellision und Boyd erfüllen. Die zweite Eigenschaft, dass das System eine Möglichkeit zum Ausdrücken von Beziehungen besitzen muss, schließt Plattformen wie Youtube aus, welche in anderen Definition, wie von der Datta et al. [21], als soziales Online-Netzwerk gezählt werden.

Für diese Arbeit wird eine Definitionen für soziale Netzwerke benötigt, die dezentrale soziale Netzwerke nicht auszuschließt, weshalb die Definition von Ellison und Boyd geeignet ist und verwendet werden kann. Allerdings wird diese Definition um den Aspekt erweitert, dass soziale Netzwerke nicht web-basiert sein müssen, da aktuelle Forschungsansätze mittels mobiler Ad-Hoc Netze soziale Netzwerke ohne Verwendung des Internets aufbauen können. Diese Art von sozialen Netzwerken stehen zwar nicht im Kern dieser Arbeit, sollen allerdings nicht ausgeschlossen werden. Aus diesem Grund und der Tatsache, dass in dieser Arbeit häufig ein Begriff für soziale Netzwerke benötigt wird, wird im weiteren Verlauf dieser Arbeit hierfür der Begriff *soziales Netzwerk* gewählt.

2.2 Klassifikation von sozialen Online-Netzwerken

Der vorherige Abschnitt zeigt, dass soziale Netzwerke verschiedene Funktionen besitzen und in unterschiedliche Ausprägungen vorkommen. Um einen besseren Überblick zu erhalten, wird nun eine Klassifikation von sozialen Online-Netzwerken vorgestellt. Hierfür gibt es mehrere Möglichkeiten, wie unter anderem die Einordnung nach der Anwendungsdomäne[5], der Region, Anzahl von Teilnehmern, Infrastruktur oder Art des Mediums.[6] Die Klassifikation von Datta et al. [21] unterscheidet soziale

[5] Unterscheidungen hierbei könnten Bildung, Dating, Games, Arbeit bzw. Jobs und Hobbys sein.
[6] Beispielsweise Videos bei Youtube

Online-Netzwerke mittels zwei Dimensionen (siehe Abbildung 1), wobei die erste die Verteilung der Infrastruktur in zentrale, verteilte und Peer-to-Peer-Infrastrukturen vornimmt. Die zweite Dimension bezieht sich auf die Möglichkeiten, die der jeweilige Dienst anbietet. Die Klassifizierung von Datta et al. wird in dieser Arbeit vorrangig behandelt, da die Infrastruktur einer der thematischen Schwerpunkte der Zielstellung ist.

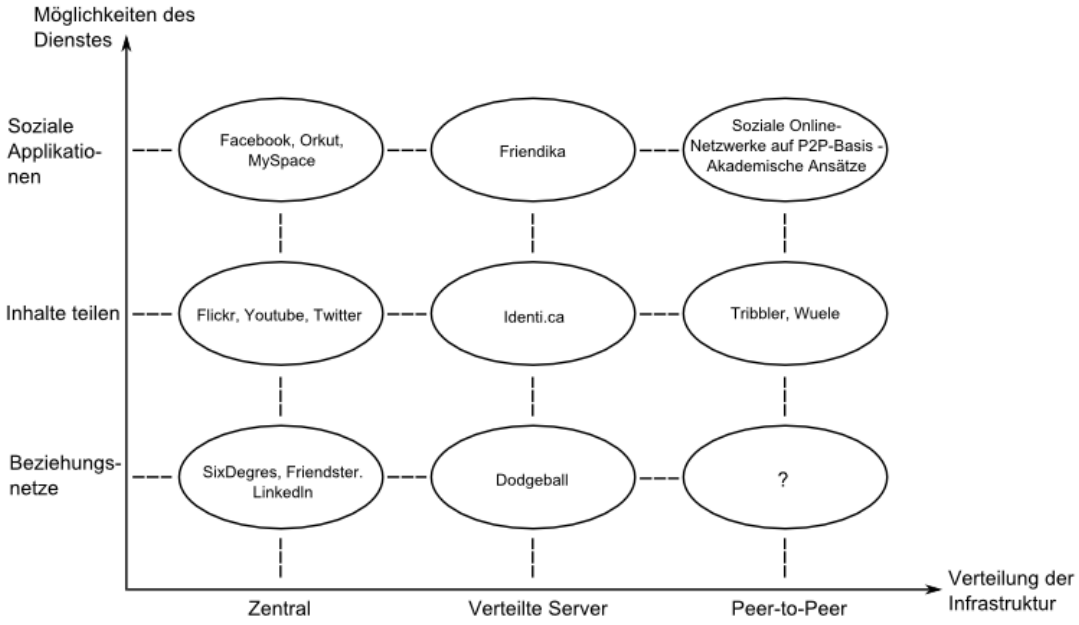

Abbildung 1: Klassifikation von sozialen Online-Netzwerken modifiziert aus [21]

Für die erste Dimension (waagerechte Achse in der Abbildung) ist die Kategorie *Zentral* für soziale Online-Netzwerke gesondert zu betrachten. Denn soziale Online-Netzwerke werden meist von einem Dienstanbieter angeboten, wie es Beispielsweise bei Facebook und Facebook Inc., Google+ und Google Inc. oder Xing und Xing AG der Fall ist. Für die Nutzer erscheinen diese Dienste jeweils als ein kohärentes System, da sie über eine einheitliche Oberfläche oder API verwendet werden. Die Infrastruktur dieser Dienste wird allerdings in vielen Fällen nicht durch einen zentralen Anwendungsserver realisiert, sondern durch das Betreiben einer verteilten Infrastruktur mit mehreren Servern gegebenenfalls auch an verschiedenen Standorten, da die Dienste auf unterschiedlichen Kontinenten verfügbar sind, hohe Lasten bewältigen müssen und bis zu einem gewissen Grad Ausfallsicherheit garantieren. In der Arbeit von Datta et al. werden sozialen Online-Plattformen eine zentrale In-

frastruktur zugesprochen, da diese die Teilnehmer- und Anwendungsdaten zu einem zentralen Archiv zusammenführen. Im weiteren Verlauf der Arbeit wird zur besseren Differenzierung dieses Aspektes auch die Formulierung soziales Netzwerk mit bzw. ohne eine zentrale Organisationseinheit verwendet. Demnach wird bei den zwei weiteren Kategorien die Infrastruktur der Plattformen nicht mehr von einer Organisationseinheit betrieben, sondern von mehreren Anbietern. Bei einer Infrastruktur mit verteilten Servern, nutzen die Teilnehmer die Plattformen weiterhin über einen oder mehrere Server, während in der letzten Kategorie (Peer-to-Peer) jeder Teilnehmer mit seinem Endgerät selbst zu einem gewissen Teil Betreiber des sozialen Netzwerkes werden kann. Der Aspekt der Dezentralisierung von sozialen Netzwerken und der dazugehörige technische Hintergrund wird in Kapitel 5 behandelt.

In der zweiten Dimension (senkrechte Achse in der Abbildung) der Klassifizierung von Datta et al. werden die Dienste nach Plattformen für das Führen von sozialen Beziehungen, Plattformen für das Teilen von Inhalten und sozialen Plattformen mit Applikationsentwicklungen unterschieden. Unter die erste Kategorie fallen nach Datta et al. Plattformen, die vornehmlich das Pflegen und Erschließen sozialer Beziehungen und das Teilen von Informationen anbieten, welche meist aus der Anfangszeit sozialer Netzwerke stammen. Die nächste Kategorie umfasst Plattformen, die auf die Teilung von Information, teilweise mit der Spezialisierung auf ein Medium ausgelegt sind. Diese Eigenschaft kann beispielsweise dazu verwendet werden Mikroblogdienste von der obersten Kategorie abzugrenzen, auch wenn sie die Eigenschaften für die zweite Kategorie erfüllen. Plattformen, die eine Vielzahl an verschiedenen Anwendungen und Diensten bereitstellen sowie das Entwickeln von Anwendungen für Drittanbieter ermöglichen, fallen in die Kategorie *Soziale Applikationen*.

2.3 Funktionen und Begriffe in sozialen Netzwerken

Da verschiedene Forschungsarbeiten aus dem Bereich sozialer Netzwerke in Kapitel 4 behandelt werden, ist es hilfreich grundlegende Funktionen und Begriffe aktueller Plattformen zu kennen. Aus diesem Grund werden die für diese Arbeit wichtigen Funktionen aufgeführt, wobei der Fokus auf die zwei Plattformen Twitter und Facebook gelegt wird.

Facebook bietet eine Reihe von Funktion, welche unter anderem in der Definition von sozialen Netzwerken genannt wurden. Dabei ist das Eingehen von sozialen Beziehungen zwischen den Teilnehmern in Facebook bidirektional geregelt und wird *Freundschaft* genannt. Eine weitere wichtige Funktion ist das Teilen von Inhalten.

Hierbei kann ein Teilnehmer einen Beitrag, bestehend aus Text, Links, Bildern oder anderen Medien auf seiner Pinnwand hinterlassen. Eine Pinnwand ist eine zu einem Teilnehmer zugehörige Seite, auf der Einträge gesammelt werden, die durch den Teilnehmer selbst und andere berechtigte Teilnehmer verfasst wurden. Die Einträge einer Pinnwand sind für andere Teilnehmer, je nach der Privatsphäreneinstellung sichtbar. Das Verfassen eines neuen Beitrages kann zur Folge haben, dass dieser in dem Newsfeed anderer Teilnehmer erscheint. Ein Newsfeed stellt kürzlich stattgefundene Aktionen anderer Teilnehmer für einen Teilnehmer dar. Damit die Aktionen der Teilnehmer in einem Newsfeed angezeigt werden, müssen diese Teilnehmer abonniert werden, was in Facebook über das Eingehen einer Freundschaft erreicht wird. Ebenso werden die Aktionen von nicht befreundeten Teilnehmern angezeigt, wenn diese öffentlich mit befreundeten Teilnehmern interagieren. Dies kann passieren, wenn andere Teilnehmer die Beiträge eines Teilnehmers kommentieren oder eigene Beiträge hinterlassen. Ebenso besteht über die *gefällt mir*-Funktion die Möglichkeit, die Sympathie für einen Beitrag auszudrücken. Allerdings bezieht sich die *gefällt mir*-Funktion nicht nur auf die Beiträge eines Teilnehmers, sondern sie kann auch bei Seiten von Organisationen oder Firmen sowie Fanseiten verwendet werden. Eine weitere Funktion ist das Anlegen von Fotoalben und Hochladen von Bildern, welche wiederum auch von den anderen Teilnehmern eingesehen, kommentiert oder mit *gefällt mir*-Angaben versehen werden können.

Die zweite Plattform Twitter ist ein Mikroblogdienst, was von Böhringer und Richter [11] als ein kleinere Version eines Blogs mit sozialen Netzwerkfunktionen beschrieben wird. Twitter bietet ähnlich wie die Pinnwand von Facebook eine *Timeline*. Der Unterschied hierbei ist, dass die Beiträge in einer Timeline auf 140 Zeichen pro Beitrag begrenzt sind und diese Beträge *Tweets* genannt werden. Damit ein Teilnehmer Tweets in seinem Newsfeed angezeigt bekommt, muss er andere Teilnehmer abonnieren, wodurch er zu einem *Follower* von dem jeweiligen Teilnehmer wird. Diese soziale Beziehung ist unidirektional, da das Folgen eines Teilnehmers nicht automatisch dazu führt, dass der andere Teilnehmer seinem Follower folgt. Des Weiteren bietet Twitter an, Tweets auf der Timeline an andere Teilnehmer über ein @ zu adressieren. Somit können öffentliche Diskussionen geführt werden. Ebenso ist es möglich mittels eines *#-Tags* ein Tweet einem Thema zu zuordnen. Dies kann beispielsweise dazu verwendet werden, um nach Tweets zu einem Thema zu suchen.

2.4 Schutzziele

Die Schutzziele der IT-Sicherheit werden nach Cutillo et al. wie folgt definiert:

> *„Security objectives are requirements that have to be satisfied in order to protect the system from potential threats and attacks."* [19]

Im Folgenden werden einige der Schutzziele näher beschrieben und ihre Bedeutung für diese Arbeit und im Bezug für Teilnehmerdaten in sozialen Netzwerken festgelegt.

Authentizität Die Anforderung nach Authentizität wird bei Eckert als die *„[...] Glaubwürdigkeit und Echtheit eines Objektes bzw. Subjektes, die anhand einer eindeutigen Identität und charakteristischen Eigenschaft überprüfbar ist"*, [28, S. 6-7] bezeichnet. In sozialen Netzwerken sind die Subjekte die Teilnehmer und Anbieter und die Objekte die Daten, die über die Teilnehmer entstehen. Damit die Authentizität der Teilnehmer sichergestellt werden kann, werden oftmals Authentifizierungen mittels eines Benutzernamen und Passwortes, die zu einem Account gehören, verwendet. Für Daten wird die Authentizität meist durch einen Urhebernachweis erbracht [28, S. 6-7]. Da Daten auch zwischen mehreren Parteien übertragen werden, gilt hierbei das Interesse des Empfängers, dass der Autor einer Nachricht authentisch ist und die Nachricht einem direkten oder indirekten Nachweis darüber beinhaltet, dass es sich dabei um den angegebenen Autor handelt [10, S. 42]. Die Authentifizierung muss sich allerdings nicht auf den Urhebernachweis beschränken. Eckert merkt hierbei in einem Beispiel an, dass auch der Nachweis über eine korrekte Funktionalität ein wichtiges Kriterium für die Echtheit eines Objektes sein kann. Im Bezug auf die Datenobjekte, die Teilnehmerdaten in einem sozialen Netzwerk repräsentieren, stellt sich die Frage, ob es hier auch spezifische Eigenschaften gibt, die für die Echtheit der Daten und somit für die Authentizität relevant sind. In Kapitel 4 wird auf diese Frage eine Antwort gegeben.

Integrität Unter Integrität wird verstanden, dass Daten vor unautorisierten Veränderungen geschützt werden und keine unbemerkten Änderungen vorgenommen werden können [28, S. 7-8]. Für soziale Netzwerke heißt das, dass Teilnehmerdaten und Nachrichten nur von den Teilnehmern oder Systemkomponenten, die berechtigt sind, modifiziert werden dürfen. Um dies zu ermöglichen, muss festgelegt sein, welche Teilnehmer oder Komponenten Schreibzugriff auf welche Daten haben. Ein Beispiel hierfür kann ein Teilnehmer sein, der ein Profil besitzt und Informationen unter diesem Profil über eine Pinnwand veröffentlich. Sobald ein anderer Teilnehmer, der

mit dem Eigentümer der Pinnwand in Beziehung steht und somit eine entsprechende Berechtigung besitzt, einen Beitrag hinterlässt, hat dieser auch die Berechtigung den Beitrag zu ändern. Der Teilnehmer, dem die Pinnwand gehört, hat dagegen in der Regel keine Berechtigung, diesen Beitrag zu editieren, darf ihn aber von seiner Pinnwand entfernen oder ausblenden. Es ist also eine Zugriffskontrolle für das Verändern von Daten erforderlich.

Verbindlichkeit Unter dieser Anforderung wird nach Eckert die Zuordenbarkeit von Aktionen verstanden, welche gewährleistet ist, wenn ein Subjekt die Durchführung der Transaktion nicht abstreiten kann. Für soziale Netzwerke bedeutet dies, dass beispielsweise sichergestellt sein muss, wenn ein Teilnehmer eine Nachricht an einen anderen Teilnehmer verschickt, dieser nicht bestreiten kann, dass die Nachricht von ihm stammt. Andersherum soll der Teilnehmer nicht abstreiten können, dass er diese erhalten hat, wenn sie ihm zugestellt wurde. Innerhalb dieser Arbeit wird das Kriterium dieses Schutzziels für den Aspekt verwendet, dass jemand nachweisen kann, dass eine Aktion stattgefunden hat. Dies überschneidet sich auch mit dem Kriterium zur Erfüllung des Schutzziels Authentizität, wenn man die Gewissheit der Durchführung einer Aktion als charakteristische Eigenschaft eines Datenobjektes von Teilnehmerdaten anwendet.

Verfügbarkeit Die Verfügbarkeit in sozialen Online-Netzwerken bedeutet, dass die Funktionsweise des Dienstes auch gegenüber Angriffen und Fehlern gegeben ist [19]. Die Funktionsweise eines Dienstes kann allerdings auch durch lange Wartezeiten bei Zugriffen über das Netzwerk mit einer geringen Bandbreite oder durch eine stark beanspruchte Ressource, beinträchtig sein. Diese führt nicht zur Verletzung des Schutzziels Verfügbarkeit, solange sich die Verzögerungen in einem angemessenen zeitlichen Rahmen befinden. In dezentralen sozialen Netzwerken wird die Verfügbarkeit mit der Fähigkeit, dass autorisierte Teilnehmer, möglichst jederzeit, auf Teilnehmerdaten anderer Teilnehmer zuzugreifen können, verbunden. Dieses Schutzziel stellt oft eine wichtige Anforderung in sozialen Netzwerken und eine große Herausforderung für einige Formen von sozialen Netzwerken dar, die über keine zentrale Organisationseinheit verfügen. Allerdings gehört die Verfügbarkeit nicht zu den Kernthemen dieser Arbeit.

Vertraulichkeit und Privatsphäre Das Schutzziel der (Informations-) Vertraulichkeit ist nach Eckert erreicht, wenn keine unautorisierte Informationsgewinnung

ermöglicht wird. Im Bezug auf soziale Netzwerke muss allerdings berücksichtig werden, dass es sich um Personenbezogene Daten handelt, weshalb hierbei häufig der Begriff Privatsphäre statt Vertraulichkeit verwendet wird. Nach Westin [65, S. 7] ist die Privatsphäre ein Anspruch darauf, dass jedes Individuum, Gruppe oder Institution selbst bestimmen kann, wie, wann und welche Informationen über einen selbst zu anderen gelangen. In diesem Sinne kann ein Teilnehmer eines sozialen Netzwerkes entscheiden, wer auf welche Informationen, wie beispielsweise Beiträge auf seiner Pinnwand Zugriff hat, was wiederrum zur Zugriffskontrolle für das Lesen von Daten führt. Zu diesem Aspekt der Privatsphäre in sozialen Netzwerken kommen nach Zhang et al. [71] das Verbergen der Identität der Teilnehmer, welche unter dem Konzept der Anonymität bekannt ist, sowie das Verbergen von Metadaten der Kommunikation für Dritte hinzu. Letzteres besagt somit, dass nicht nur Kommunikationsinhalte, sondern sämtliche Metadaten, wie der Zeitpunkt, Teilnehmer und die Länge der Kommunikation zu schützen sind. Des Weiteren zählen hierzu Informationen, die das Verhalten der Teilnehmer betreffen, welche beispielsweise ein Dienstanbieter eines sozialen Netzwerkes erfassen kann, wie Anmeldezeitpunkte an dem System oder Profile, die ein Teilnehmer aufgerufen hat. Ein Dienstanbieter, der auf die Informationen seiner Teilnehmer zugreift, erfüllt in der Regel die Kriterien der Vertraulichkeit, da er von dem Teilnehmer über die Einwilligung der Nutzungsbedingungen dazu autorisiert wurde, verletzt dabei aber die Kriterien zum Schutz der Privatsphäre. Somit umfasst die Privatsphäre die Anforderung der Vertraulichkeit, schafft aber auch weitere Merkmale, wie die der Anonymität oder das Verbergen von Informationen gegenüber dem Dienstanbieter. Der Schutz der Privatsphäre gehört nicht zum Kernthema dieser Arbeit, da sie allerdings nicht selten die primäre Motivation zur Nutzung und Entwicklung eines sozialen Netzwerkes ohne eine zentrale Organisationseinheit ist, wird sie in weiteren Diskussionen gegebenenfalls berücksichtig.

2.5 Vertrauen, Reputation und Glaubwürdigkeit

In den späteren Kapiteln wird von den Begriffen *Vertrauen*, *Reputation* und *Glaubwürdigkeit* vermehrt Gebrauch gemacht, weshalb in diesem Abschnitt einige Definitionen zu diesen Begriffen vorgestellt werden.

Vertrauen ist ein Konzept, welches auch im realen Leben und in vielen Forschungsfeldern Anwendung findet, wie unter anderem in der Psychologie, Soziologie, Ökonomie, Philosophie und Informatik. Dieses weitreichende Konzept wird in den

jeweiligen Disziplinen unterschiedlich definiert [17], wobei an dieser Stelle aufgrund des thematischen Schwerpunktes der Fokus auf die Definitionen gelegt wird, die sich im Bereich der sozialen Netzwerke verwenden lassen.

Eine Definition für Vertrauen von Internetanwendungen stammt von Grandison und Sloman [33] und lautet:

> „*[...] the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context*", [33]

Diese Definition lässt sich auch für soziale Netzwerke verwenden, wobei sich hier das Vertrauen von einem Teilnehmer hin zu einem Anbieter des sozialen Netzwerkes beschreiben lässt. Die Teilnehmer haben die Möglichkeit darauf zu vertrauen, dass der Anbieter seine Befugnisse nicht missbraucht oder die ihm anvertrauten Daten nicht ohne Zustimmung der Teilnehmer an Dritte weiter gibt. Ebenso kann ein Teilnehmer in die Zuverlässigkeit eines Dienstes hinsichtlich seiner Verfügbarkeit und der Sicherheit im Bezug auf den Schutz seiner Daten vertrauen. Dieses Vertrauen ist aber nicht zwangsläufig gegeben, weshalb eine Person eine Abneigung gegenüber der Nutzung eines sozialen Netzwerkes besitzen kann. In sozialen Netzwerken besteht Vertrauen aber nicht nur zwischen einem Dienstanbieter und seinen Teilnehmern, sondern auch zwischen den Teilnehmern untereinander. Dieses Vertrauen wird von Golbeck [30] wie folgt beschrieben:

> „[...] *trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome.*", [30]

In sozialen Netzwerken kann diese Art des Vertrauens auch über die eingegangenen sozialen Beziehungen der Teilnehmer untereinander abgeleitet werden. Ein Teilnehmer der beispielsweise einem anderen Teilnehmer bei Twitter folgt, vertraut möglicherweise darauf, dass dieser interessante und wissenswerte Informationen verbreitet. Eine andere Möglichkeit ist, dass zwischen den beiden Teilnehmern auch im realen Leben eine soziale Beziehung besteht. Die Annahme, dass sich Teilnehmer, zwischen denen eine soziale Beziehungen besteht, entsprechend der Definition von Golbeck verhalten, kann auch für das Design von sozialen Netzwerken verwendet werden [20, 66]. Diese Art des Vertrauens wird im weiteren Verlauf als *soziales Vertrauen* bezeichnet. Golbeck spricht sozialem Vertrauen drei Eigenschaften zu, nämlich Transitivität, Asymmetrie und Personalisierung. Ausführlich heißt dies, dass Vertrauen zwischen zwei Personen nur bedingt transitiv ist. Beispielsweise kann Alice Bob und Bob Charlie vertrauen, was aber nicht gleichzeitig bedeutet, dass Alice

auch Charlie vertraut. Vertrauen kann nach Golbeck über Empfehlungen zwischen Personen ausgetauscht werden, was zu der Unterscheidung zwischen dem Vertrauen in eine Person und in der Empfehlung einer Person führt. Der zweite Punkt sagt aus, dass Vertrauen nicht bidirektional sein muss. Der dritte Punkt umfasst, dass die Ansicht, ob eine Person vertrauenswürdig ist, von Person zu Person unterschiedlich sein kann. Somit ergibt sich, dass Vertrauen abhängig von der jeweiligen Person ist.

Ein weiteres Konzept, dass mit Vertrauen im Zusammenhang steht ist Reputation. Reputation kann nach Rahman et al. [2] verallgemeinert als die Annahme darüber, wie sich eine Entität verhalten wird, basierend auf den Informationen über das vorangegangene Verhalten der Entität, verstanden werden. Die Informationen über vorangegangenes Verhalten müssen dabei nicht zwangsläufig von einem Teilnehmer selbst, sondern können auch von anderen Teilnehmern kommen. Ein bekanntes Reputationssystem komm bei Ebay[7] zum Einsatz. Hierbei können sich der Käufer und Verkäufer gegenseitig nach einer Transaktion bewerten. Andere Teilnehmer können anhand dieser Bewertung entscheiden, ob sie mit einem anderen Teilnehmer zukünftige Transaktionen durchführen wollen.

Als letztes gilt es noch den Begriff *Glaubwürdigkeit* zu erläutern. Hierbei gibt es Definitionen, die diesen Begriff im Kontext eines bestimmten Forschungsfeldes festlegen oder versuchen allgemeine Gültigkeit zu erreichen. Die Definition aus dem Merriam-Webster Lexikon nennt einen allgemein gültigen Ansatz und beschreibt Glaubwürdigkeit als „*the quality of being believed or accepted as true, real, or honest*" [45]. Hilligos und Rieh stellen in [36] fest, dass die übergreifende Sicht in den Arbeiten von Kommunikationsforschern für Glaubwürdigkeit die Glaubhaftigkeit ist. Selbst definieren sie Glaubwürdigkeit als den Hauptaspekt von Informationsqualität. Die Informationsqualität wird von ihnen als das subjektive Empfinden hinsichtlich der Qualität und Nützlichkeit einer Information bezeichnet.

Die Forschungfeldspezifischen Ansätze, die an dieser Stelle vorgestellt werden, stammen aus dem Bereich der Glaubwürdigkeitsbestimmung in sozialen Netzwerken. Castillo et al. [15] sprechen hierbei von *social media credibility*, welche als die Informationsglaubwürdigkeit verstanden wird, die sich nur mit Informationen aus der Social Media Plattform bestimmt lässt. Gupta et al. [34] dagegen definieren Glaubwürdigkeit bezüglich eines Events in Twitter als Grad mit dem ein Teilnehmer einem Event Glauben schenken kann, wenn er eine Reihe von Tweets von diesem Event überflogen hat. Das Event selbst besteht somit aus der Glaubwürdigkeit der dazugehörigen Tweets. Ebenso wird die Glaubwürdigkeit eines Teilnehmers anhand

[7] www.ebay.com, letzte Sichtung 30.11.2013

der Tweets die er zur Verfügung stellt festgemacht. Die Glaubwürdigkeit des Tweets selbst ist abhängig von dem Event, dem Teilnehmer und der Glaubwürdigkeit anderer Tweets, die eine ähnliche Aussage machen. Abschließend bleibt hier festzuhalten, dass der Begriff *Glaubwürdigkeit* durch den Kontext bestimmt sein kann, in dem er verwendet wird.

2.6 Zusammenfassung

Dieses einleitende Kapitel wurde dazu verwendet, erste Begriffe und Definitionen anzuführen. Hierbei wurde auf die Begriffe Glaubwürdigkeit, Reputation und Vertrauen eingegangen. Des Weiteren wurde der Begriff soziale Netzwerke, eine Einteilung von sozialen Netzwerken und eine Auswahl von grundsätzlichen Funktionen vorgestellt. Danach wurden die Schutzziele aus der IT-Sicherheit und ihre Relevanz für diese Arbeit dargelegt.

3 Situations- und Angriffsbeschreibung

Ziel dieses Kapitel ist es, mögliche Angriffe auf die Integrität und Authentizität der Teilnehmerdaten zu identifizieren. Um dies zu erreichen, werden zuerst die Ausgangssituation und die Interessengruppen mit ihren Anreizen beschrieben. Da die Gefahr besteht, Angriffe zu übersehen oder zu vernachlässigen, die sich bei der Konzeption von sozialen Netzwerken oder Sicherheitsmechanismen als wesentlich erweisen, werden die Anreize der Angreifer erst allgemein für dezentrale soziale Netzwerke beschrieben. Dies führt dazu, dass auch Angriffe identifiziert werden, die unerheblich für die weitere Bearbeitung dieser Masterthesis sind. Aus diesem Grund erfolgt im Anschluss eine Diskussion der relevanten Angriffe hinsichtlich der Zielstellung. Diese Betrachtung bietet noch nicht die Möglichkeit detailliert auf technische Lösungen und Schwächen einzugehen, weshalb es ein weiteres Ziel ist, die relevanten Bereiche zu identifizieren, die in den vertiefenden Kapiteln behandelt werden.

3.1 Ausgangssituation

Für diese Arbeit wird davon ausgegangen, dass soziale Netzwerke, unabhängig ob diese mit oder ohne einer zentralen Organisationseinheit betrieben werden, von einer ausreichenden Anzahl an Teilnehmern verwendet werden. Des Weiteren existieren Verfahren, die es ermöglichen, einen Beitrag eines Nutzers einem Thema zuzuordnen, Beiträge nach ihrer Glaubwürdigkeit einzustufen und Teilnehmer hinsichtlich ihres Verhaltens als Spammer[8] zu erkennen. Die Beiträge, Diskussionen und Inhalte, die innerhalb der sozialen Netzwerke ausgetauscht werden, bestehen zu einem wesentlichen Anteil aus sensiblen Daten und sind somit schützenswert. Die technische Infrastruktur und die Teilnehmer des sozialen Netzwerkes sind dabei nicht auf ein Land begrenzt. Die Kommunikationsinfrastruktur der jeweiligen Länder, welche allerdings gegebenenfalls überwacht wird, ist in Takt. Ebenso können zentral verwaltete Systeme der Zensur unterliegen und überwacht werden. Die sozial-politische Situation, in den die Teilnehmer des Netzwerkes leben, sind durch zwei Merkmale gekennzeichnet:

1. Die Menschen des jeweiligen Landes verfügen weitestgehend Meinungsfreiheit und müssen nicht mit der Verfolgung aufgrund ihrer Äußerungen und Taten durch die Regierung rechnen. Davon ausgenommen sind extreme Handlungen,

[8] siehe auch http://www.merriam-webster.com/dictionary/spam, letzte Sichtung 30.11.2013

die sich gegen die gesellschaftlichen und kulturellen Regeln des Landes richten. Die klassischen Medien wie Fernsehen, Radio und Zeitung können zumindest teilweise unabhängig Berichten.

2. Für Äußerungen und Handlungen, die nicht den Maßstäben der jeweiligen Regierung des Landes entsprechen, müssen die Menschen in diesem Land mit Repressionen rechnen. Klassische Medien bringen kaum oder gar keine kritische Berichterstattung über das Vorgehen der Regierung.

3.2 Interessengruppen und Anreize

Die Interessengruppen lassen sich für die oben beschriebene Ausgangssituation in die Gruppe der aufrichtig Beteiligten und der Angreifer unterteilen. Aufrichtig Beteiligte umfassen hierbei Teilnehmer des sozialen Netzwerkes und je nach Grad der Dezentralisierung, Anbieter bzw. Organisationseinheiten von sozialen Netzwerken, welche in ihrem Handeln nicht bösartig agieren. Unter bösartiges Agieren bzw. Handeln wird hier das Zufügen von Schaden zu einer Partei, das Verschaffen von unbefugten Vorteilen für andere oder einen selbst, sowie der unbefugte Zugriff auf Ressourcen verstanden. Dabei können je nach Situation auch weitere Aspekte, wie beispielsweise das Vorgeben falscher Tatsachen, zählen. Zu den hier bereits beschriebenen Rollen können noch weitere aus der Liste der Stakeholder für soziale Netzwerke hinzukommen, wie Sponsoren oder Werbepartner. Diese können sich ebenso aufrichtig oder bösartig verhalten, allerdings werden diese nicht weiter besprochen, da in sozialen Netzwerken ohne eine zentrale Organisationseinheit der Fokus meist auf den vorher genannten Rollen liegt.

Die Gruppe der Angreifer bezieht sich zum einen auf Beteiligte des sozialen Netzwerkes, wie legitimierte Teilnehmer und Dienstanbieter, welche sich allerdings bösartig Verhalten. Ebenso kann ein Angreifer auch aus einer externen Position agieren und muss deshalb nicht zwangsläufig ein Teilnehmer des sozialen Netzwerkes sein. Die Angriffe können auf verschiedenen Ebenen eines sozialen Netzwerkes durchgeführt werden, welche in Abbildung 2 nach dem Modell von [20] dargestellt sind. Die Ebenen werden in die soziale Netzwerk-, Anwendungs- sowie Kommunikations- und Transportebene unterteilt. Die soziale Netzwerkebene beinhaltet die Funktionalitäten, wie das Erstellen eines Profils oder das Eingehen von Freundschaften, wie bereits in Abschnitt 2.1 beschrieben. Auf der Anwendungsebene befindet sich die Infrastruktur des sozialen Netzwerkes, die die Funktionalität für die darüber liegende Ebene ermöglicht. Unter diese Ebene liegt die Transportebene, welche die Kommuni-

kation über Netzwerkkomponenten ermöglicht, wie beispielsweise das Internet oder ein mobiles Ad-hoc Netzwerk.

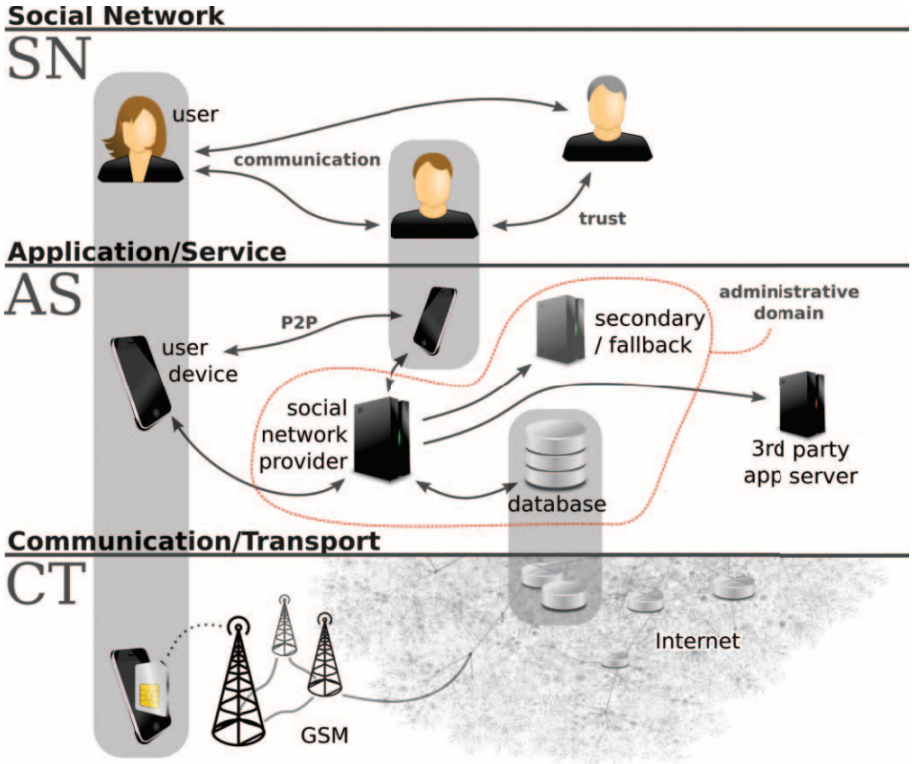

Abbildung 2: Die Architekturebenen sozialer Netzwerke aus [51]

3.2.1 Anreize und Interessen der aufrichtig Beteiligten

Die Motivation der aufrichtig Beteiligten kann je nach Anbieter eines Dienstes oder Teilnehmer variieren. Ausgehend von der ersten sozial-politischen Situation aus Abschnitt 3.1, sind die Teilnehmer zur Nutzung sozialer Netzwerke ohne zentrale Organisationseinheiten motiviert, um von deren Vorteile, welche in Kapitel 1 beschrieben sind, zu profitieren. Dabei kann der Schutz der Privatsphäre bzw. persönlicher Daten, Kompatibilität zu anderen Netzwerken sowie die Unabhängigkeit gegenüber den Vorgaben einer zentralen Organisationseinheit im Vordergrund stehen. Ebenso können auch andere Faktoren, welche unspezifisch für dezentral organisierte soziale Netzwerke sind, ausschlaggebend sein. Beispiele hierfür können eine hohe Anzahl an Freunden oder wichtigen Personen, die das Netzwerk benutzen, das Erhalten von Ansehen, der thematische Informationsgehalt oder die Qualität der Informationen

in dem Netzwerk sein. Die letzten zwei Aspekte erhalten eine höhere Relevanz für die Teilnehmer, wenn klassische Medien keine unabhängige Berichterstattung bieten. Gleichzeitig besteht in dieser Situation der Bedarf nach Anonymität oder nach Schutz von persönlichen Daten, wenn die Teilnehmer beim Vertreten ihrer Ansichten mit Repressionen rechnen müssen, wenn diese nicht konform mit denen des Staates sind.

Anbieter eines sozialen Netzwerkes können hierbei Betreiber eines der verteilten Server oder ein Knoten mit besonderen Aufgaben für den Betrieb des Netzwerks sein. Die Anreize hierfür sind unterschiedlich und können unter anderem aus finanziellen Gesichtspunkten, politischen Überzeugungen oder aus Fairness heraus motiviert sein. Weitere Gründe können hierfür das Schaffen einer Community oder die Kontrolle über die eigenen Daten und Sicherheitsmechanismen sein.

3.2.2 Anreize und Interessen der Angreifer

Angreifer haben ebenso wie aufrichtig Beteiligte verschiedene Anreize, je nachdem in welcher Rolle sie agieren. Die im Folgenden aufgeführten Rollen stellen nur eine Auswahl dar und gelten nicht als Beschränkung der möglichen Rollen:

- **Ein Staat und seine Behörden** - Der Staat kann verschiedene Interessen verfolgen, je nach dem welche Regierung bzw. Behörde als Angreifer agiert. Innerhalb der ersten sozial-politischen Situation könnte ein Ziel eines Staates das Sammeln von Informationen sein, um beispielsweise terroristische Anschläge abzuwehren. Gleichzeitig verletzt der Staat damit die Privatsphäre der Teilnehmer der Netzwerke, wenn er sich Informationen über das Privatleben der Bürger verschafft, wie beim Abhören der Kommunikation. In der zweiten politischen Situation ergeben sich eine Reihe weiterer Anreize für einen Staat, wenn ein Teil der Gegenbewegung oder der Bevölkerung das soziale Netzwerk verwendet. Organisiert sich eine Gegenbewegung oder die Opposition über ein soziales Netzwerk, kann ein Staat daran interessiert sein, die Mitglieder oder Angehörige der Mitglieder dieser Bewegung aufzuspüren oder zu erkennen, einzelne Personen oder Gruppierungen zu diffamieren, die Funktionsweise des sozialen Netzwerkes einzuschränken oder komplett zu stören. Des Weiteren kann ein Staat das soziale Netzwerk für den Versuch nutzen, die Bevölkerung zu beeinflussen. Dies kann möglicherweise durch das Zensieren von Beiträgen oder das Verbreiten von Propaganda in eigener Sache erreicht werden. Ebenso kann ein Staat versuchen Stimmungen in dem Netzwerk zu beobachten, um

auf diese zu reagieren und das soziale Netzwerk für seinen Vorteil zu nutzen.

- **Egoistische Teilnehmer** - Egoistische Teilnehmer verwenden das Netzwerk mit der Motivation, einen hohen Nutzen für sich selbst zu erreichen. Hierfür können Manipulationen in dem Netzwerk durchgeführt werden, wenn diese zu ihrem Vorteil beitragen. Ein Beispiel hierzu kann das Erlangen einer unberechtigten Reputationen sein, welche mittels Manipulation des sozialen Netzwerkes erreicht wird. Der Teilnehmer kann dadurch die Vorteile der Reputation nutzen, ohne den dafür nötigen Aufwand erbringen zu müssen. Eine andere Möglichkeit besteht darin, eigene Ressourcen zur Erhaltung des Netzwerkes nicht freizugeben, um Energie oder Rechenkapazität zu sparen.[9]

- **Hacker oder Hackergruppen** - Bei einem oder einer Gruppe von Hackern können die Angriffe auf ein soziales Netzwerk durch politische Gründe, aus Spaß oder zum Erreichen von Anerkennung in der Community, motiviert sein. Dies kann Anlass für Diffamierung, den Diebstahl von Daten oder Manipulationen eines Systems sein. Ein anderer Grund kann das Auffinden von Sicherheitslücken der Systeme sein, um auf Missstände bei den Anbietern oder den Systemen hinzuweisen. Die Angriffe können aber auch einen finanziellen Hintergrund haben, wenn erbeutete Daten verkauft oder für Erpressungen genutzt werden.

- **Konkurrierende Anbieter** - Ein weiterer Angreifer kann auch ein konkurrierender Anbieter eines sozialen Netzwerkes sein, welcher aktiv versucht, das andere Netzwerk in jeglicher Form zu stören. Somit können Teilnehmer demotiviert werden, dass Netzwerk zu nutzen oder zu einem Wechsel in das eigene soziale Netzwerk motiviert.

- **Verfeindete oder misstrauische Teilnehmer** - Hierbei handelt es sich zum einen um Teilnehmer des Netzwerkes, die anderen Teilnehmern misstrauen, beispielsweise eine Person, die jemanden im eigenen sozialen Umfeld versucht auszuspionieren und zum anderen um Teilnehmer, die Antipathien zu anderen Teilnehmern haben und aktiv versuchen, diesen Teilnehmern Schaden zuzufügen.

- **Unternehmen -** Für Unternehmen kann das Sammeln von Informationen ein wichtiger Faktor sein, um beispielsweise konkurrierende Unternehmen aus-

[9] Dieser Anwendungsfall ist unter dem *free rider problem* bekannt.

zuspionieren oder die Daten der Teilnehmer für eigene Marketingzwecke zu verwenden.

- **Kriminelle Personen** - Ziel dieser Gruppe ist es, Informationen von Teilnehmer zu erbeuten und diese beispielsweise für betrügerische Tätigkeiten zu verwenden. Ein weiteres Ziel kann das Versenden von Spam sein, die Links zu Seiten mit Schadsoftware, Fishing-Angriffen oder Werbung enthalten.

3.3 Angriffsmodell

Die oben aufgeführten Anreize der Angreifer geben einen Rahmen für mögliche Angriffe, die bei der Konzeption und Umsetzung von sozialen Netzwerken zu berücksichtigen sind. Die Angriffe, die im weiteren Verlauf vorgestellt werden, umfassen in der Regel die Verletzung eines oder mehrerer Schutzziele. Um die vorrangigen Angriffe hinsichtlich der Zielstellung auszuwählen, werden diese anschließend diskutiert. Deshalb wird bei der Diskussion angenommen, dass die vorrangige Motivation der Angreifer die Manipulation der Teilnehmerdaten ist, um Verfahren auf Anwendungsebene oder Teilnehmer auf der sozialen Netzwerkebene zu täuschen. Für eine bessere Struktur der Analyse der Angriffe, erfolgt diese nach dem Modell aus [20].

3.3.1 Transport- und Kommunikationsebene

Um Angriffe auf der Transportebene durzuführen, braucht der Angreifer kein Teilnehmer des sozialen Netzwerkes zu sein. Die Angriffe können an verschiedenen Punkten ansetzen. Beispielsweise kann ein passiver Angriff das Mitlesen von Datenpaketen sein, welcher sich lokal innerhalb eines WLANs oder LANs, durch einen Internet Service Provider oder durch einen Knoten in einem MANET umsetzen lässt. Ziel dieser Angriffe ist das Erlangen von Wissen und ist somit, im Fall von sozialen Netzwerken, ein Angriff auf die Privatsphäre oder die Grundlage für weitere Angriffe.

Aktive Angriffe können nach Paul et al. [51] das Verändern oder Erzeugen von Datenpaketen sein und gefährden somit die Integrität der Daten beziehungsweise Nachrichten in dem Netzwerk. Es erfordert allerdings umfangreiches Wissen über die Gegebenheiten des Netzwerkes, um sinnvolle Pakete zu erzeugen, weshalb dieser Angriff eher unwahrscheinlich ist. Das Blockieren, Filtern oder Verzögern von Datenpaketen sind weitere Varianten von aktiven Angriffen, welche synchrone Kommunikation einschränken oder unmöglich machen. Gleichzeitig wird die Funktionsweise des Netzwerkes behindert. Eine weitere Art von Angriffen, wie Distributed-Denial-of-Service-Angriffe (DDoS), zielen auf die Verfügbarkeit eines soziale Netzwerkes

ab. Mittels eines DDoS lassen sich die Geräte eines Teilnehmers oder Netzwerkkomponenten durch eine Vielzahl an Anfragen überlasten und unterbinden somit die Funktionsfähigkeit dieser Geräte. Angriffe dieser Art können hierbei durch eine Gruppe von Personen oder einem Verbund von Rechnern, beispielsweise durch ein Botnetz, durchgeführt werden. Hat der Angreifer umfangreichen Einfluss auf die Infrastruktur einer Region, wie beispielsweise ein Staat, so kann dieser in kritischen Situation die Möglichkeit besitzen, die komplette Infrastruktur abzuschalten, um die Kommunikation zu unterbinden. Dies lässt sich unter anderem durch das Sperren von IP-Adressen oder das Einstellen einzelner Dienste, wie den Internet Service Providern (ISP), bewerkstelligen.[10]

3.3.2 Diskussion der Angriffe auf Transport- und Kommunikationsebene

Die passiven Angriffe auf Transport- und Kommunikationsebene stellen keine direkte Bedrohung für die Integrität und Authentizität dar. Ebenso betreffen die aktiven Angriffe meist die Verfügbarkeit, mit Ausnahme der Angriffe, bei denen Netzwerkpakete hinzugefügt, gefiltert oder manipuliert wird. Hierbei können allerdings auch zusätzlich die Integrität, Verbindlichkeit oder Authentizität der Nachrichten verletzt werden.

Alle Angriffe auf dieser Ebene sind unspezifisch für soziale Netzwerke und können auch in anderen Anwendungsdomänen vorkommen. Aus diesem Aspekt heraus und der bereits erwähnten geringen Eintrittswahrscheinlichkeit für erfolgreiche Angriffe mittels des Einfügen von Datenpaketen, werden Angriffe auf der Transport- und Kommunikationsebene innerhalb dieser Arbeit nicht ausführlicher behandelt. Nichts desto trotz ist es möglich, dass Datenpakete auf der Transport- und Kommunikationsebene verändert werden, weshalb in den weiteren Kapiteln die Sicherung der Integrität und Authentizität bei den Übertragungen berücksichtig wird.

3.3.3 Anwendungsebene

Ein Angreifer auf der Anwendungsebene ist im Regelfall in einer oder mehreren Formen an dem Netzwerk beteiligt, wobei diese abhängig von den möglichen Rollen des sozialen Netzwerkes sind. Beispiele für diese Rollen sind u.a. Teilnehmer, Knoten mit privilegierten Rechten bzw. besonderen Aufgaben oder Betreiber eines verteilten Servers. Die Möglichkeit zur Durchführung eines Angriffes ist somit gegebenenfalls

[10] siehe hierzu http://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/aegypten-offline-der-blackout-am-digitalen-suezkanal-1576122.html, letzte Sichtung 30.11.2013

von dem Design des sozialen Netzwerks (siehe Kapitel 5) und der jeweiligen Rolle abhängig.

Auf der Anwendungsebene können ebenso Teilnehmerdaten und der Datentransfer manipuliert, selbst erzeugt, geblockt oder gelöscht werden [51], was wiederrum zur Verletzung mehrerer Schutzziele führen kann. Die Möglichkeiten des Angreifers variieren hierbei je nach den verwendeten Verfahren zur Übertragung und Speicherung. Des Weiteren kann ein Angreifer Sicherheitslücken ausnutzen, um Angriffe dieser Art durchzuführen. Bei verteilten Servern oder Knoten mit besonderen Aufgaben, können diese ihre Berechtigungen ausnutzen, um Manipulationen vorzunehmen oder Daten mitzulesen.

Das Beobachten von Datentransfer und das Protokollieren von Änderungen an Datenobjekten, stellen eine Verletzung der Privatsphäre bzw. der Vertraulichkeit dar. Hierbei können auch verschlüsselte Daten Aufschluss über den Inhalt oder die Beziehung zwischen den Teilnehmern geben, wenn die Frequenz und Anzahl der Nachrichten oder die Größe der Nachrichten betrachtet wird. Eine andere Möglichkeit, um an Daten eines Teilnehmers zu gelangen, können schwache Privatsphäreneinstellungen eines Teilnehmers oder der Plattform sein. Ebenso können fremde Teilnehmer Informationen über einen anderen Teilnehmer erhalten, wenn diese Freundschaftsanfragen von Personen annehmen, die sie nicht kennen und sich somit Zugriffsbeschränkungen für diesen Teilnehmer aufheben. Dazu kann es vorkommen, dass beim Eingehen einer Beziehung mit einem anderen Teilnehmer zusätzlich Informationen auch für die sozialen Kontakte dieses Teilnehmers freigegeben werden. Sind die Daten des Netzwerkes öffentlich zugänglich, können auch Teilnehmer ohne eine soziale Beziehung in dem Netzwerk zu dem Teilnehmer, Informationen über den Teilnehmer sammeln und möglicherweise für weitere Angriffe verwenden. Dabei besteht, je nach sozialen Netzwerk, die Möglichkeit die öffentlichen Daten einzusehen, ohne einen Account bei dem sozialen Netzwerk zu besitzen.

Ein weiterer Angriffspunkt auf der Anwendungsebene ist nach Paul et al. das Identitätsmanagement, welches es beispielsweise erlaubt, die Identität eines anderen Teilnehmers zu nutzen oder Aktionen unter einer falschen Identität durchzuführen. Zusätzlich kann ein Angreifer viele falsche Identitäten erstellen, welche dann für den Zweck des Angreifers genutzt werden können, was unter dem Namen *Sybil-Angriff* [27] bekannt ist. Mittels Sybils lassen sich beispielsweise Statistiken manipulieren[11] oder ein Teilnehmer kann von kontrollierten Teilnehmern des Angreifers umzingelt

[11] Ein Beispiel ist hier, dass die Sybil-Accounts eine Nachricht möglichst häufig teilen, um eine höhere Reputation oder aufsehen für diese Nachricht zu erreichen.

(Eclipse-Angriff) werden. Nach Cutillo et al. [19] lassen sich diese Angriffe hinsichtlich des Identitätsmanagements aufschlüsseln in:

- Imitation einer Person - Der Angreifer erstellt ein Profil in einem sozialen Netzwerk von einer real existierenden Person, die selber über kein Profil in dem gleichen sozialen Netzwerk verfügt.
- Klonen des Profils - Der Angreifer erstellt ein Profil einer Person, in einem sozialen Netzwerk, in dem die Person schon angemeldet ist.
- Portierung des Profils - Eine Kopie eines Profils einer Person aus einem sozialen Netzwerk wird in einem anderen sozialem Netzwerk von dem Angreifer erstellt.
- Profil Hijacking - Der Angreifer verschafft sich Zugang zu dem Profil eines Nutzer über das Aushebeln von Sicherheitsmechanismen, Social Engineering oder Erraten des Passworts. Dieser Angriff erfolgt somit auch auf der sozialen Netzwerkebene.
- Identitätsdiebstahl - Der Angreifer verschafft sich Zugang zu einem Profil (siehe Profil Hijacking) und verwendet diese für seine Zwecke bzw. nutzt dessen Reputation. Alternativ gibt ein Angreifer vor Inhaber eines Profils zu sein und führt die Konversation über andere Kanäle als dem sozialen Netzwerk.

Die Methoden zur Spamerkennung und Glaubwürdigkeitsbestimmung aus der oben beschrieben Ausgangssituation bringen einen weiteren Angriffspunkt mit sich, da ein Angreifer auch Versuchen kann, diese Verfahren für seine eigenen Zwecke zu nutzen. Bei einer entsprechenden Manipulation könnte ein Angreifer deshalb seine eigenen Beiträge glaubwürdiger erscheinen lassen, als sie wahrheitsgemäß sind oder andere Teilnehmer fälschlicher Weise als Spammer kennzeichnen lassen, während eigene Spamaccounts unberührt bleiben. Dies kann über die Manipulation von Teilnehmerdaten oder über die Anpassung des eigenen Verhaltens an die Erkennungsmechanismen dieser Methoden erreicht werden.

3.3.4 Diskussion der Angriffe auf Anwendungsebene

Ein offensichtlicher Angriff auf die Integrität und Authentizität ist die unautorisierte und teils auch autorisierte Manipulation der Teilnehmerdaten und das Einschleusen von Nachrichten auf der Anwendungsebene. Wie oben bereits beschrieben, gibt es Angriffe, die die Schwachstellen der Komponenten auf Anwendungsebene ausnutzen.

Um ermitteln zu können, an welchen Stellen diese Angriffe ansetzen können, ist es hilfreich, die Subjekte und Objekte des zu schützenden Systems und ihre Anforderungen hinsichtlich der Schutzziele Authentizität und Integrität zu sammeln. Bei den Subjekten handelt es sich bei sozialen Netzwerken um die Teilnehmer, bestehend aus Institutionen und Nutzern, welche einen Account und somit eine eindeutige Kennung in dem System besitzen. Des Weiteren kommen je nach der Infrastruktur des sozialen Netzwerkes die Anbieter dazu. Diese können auch durch ein System vertreten werden. Die Objekte sind die zu schützenden Daten eines jeden Teilnehmers. Somit lassen sich folgenden Anforderungen nennen:

1. *Ist das Subjekt, welches eine Aktion durchführt, hinsichtlich der verwendeten Identität authentisch?*
   Dies entspricht den Kriterien aus Abschnitt 2.4, nämlich dass ein Subjekt, welches in Form einer autonom agierenden Maschine (Beispielsweise der Server des Anbieters) oder einer Person, eine eindeutige Identität in dem System besitzt, die überprüfbar ist. Hiermit sind Anforderungen an die Authentifizierungsmaßnahmen verbunden.

2. *Ist das Subjekt berechtigt die Aktion durchzuführen?*
   Ein Subjekt, welches lesende oder schreibende Zugriffe auf die Daten eines Teilnehmers durchführt, muss eine entsprechende Berechtigung besitzen. Dies ist zum einen für den Schutz der Integrität wichtig, allerdings auch für die Authentizität, da unberechtigte Veränderung die Daten verfälschen können. Lesende Zugriffe beziehen sich dabei auf die Anforderung nach der Vertraulichkeit bzw. Privatsphäre. Um dies zu ermöglichen ist das Umsetzen von Zugriffskontrollen notwendig.

3. *Wurden die Nachrichten auf dem Weg zum Ziel nicht verändert?*
   Dieser Aspekt bezieht sich auf die Nachrichtenintegrität, die auf dem Übertragungsweg verletzt werden kann.

4. *Wurden Manipulationen an den persistenten Teilnehmerdaten korrekt durchgeführt?*
   Da die Daten eines Teilnehmers möglicherweise nicht auf seinem eigenen Gerät, sondern auf den Endgeräten anderer Teilnehmer oder den Servern der die Dienstanbieter liegen, führt der Teilnehmer eine Änderung an seinen Daten nicht selbst durch, sondern gibt diese in Auftrag. Hierbei ist zu beachten, dass

das System garantiert, dass eine Manipulation so durchgeführt wird, wie sie von dem Teilnehmer vorgegeben wurde.

5. *Wird durch die durchgeführte Aktion die Echtheit des Objektes gewährleistet?* Dieser Punkt bezieht sich darauf, dass die Daten in sozialen Netzwerken hinsichtlich der repräsentierten Information auch einen Zweck erfüllen. Es ist somit nicht ausreichend, dass ein Teilnehmer eine autorisierte Manipulation vornimmt, wenn die eigentliche Information dadurch verloren oder verfälscht wird. Dies kommt beispielsweise vor, wenn ein Teilnehmer die Informationen in seinem Profil selbst gestalten kann und somit auch Kommentare zu seinen Beiträgen erzeugen kann. Um diesen Punkt zu adressieren, muss ermittelt werden, welche Datenobjekte in sozialen Netzwerken Eigenschaften besitzen, bei denen geprüft werden muss, ob eine Änderung zu einem weiterhin authentischen Datenobjekt führt.

6. *Ist die Instanz, die die Aktion durchführt, hinsichtlich einer realen Identität authentisch?*
   Hiermit wird das Problem adressiert, dass durch die Erstellung von falschen Identitäten Teilnehmerdaten manipuliert werden können, beispielsweise durch eine Sybil-Attacke. Eine reale Identität kann eine Person, Firma, Organisation und so weiter sein. Es muss hier allerdings bedacht werden, dass ein Interessenkonflikt mit der Privatsphäre entstehen kann, da Menschen mehrere digitale Identitäten verwenden können, um beispielsweise ihre privaten und beruflichen Aktivitäten zu trennen. Dies ist eine Anforderung an das Identitätsmanagement und sollte berücksichtigt werden.

Auch wenn die sechs genannten Punkte erfüllt werden, ist es möglich, dass die Verfahren auf Anwendungsebene, wie Spam-Erkennung und Glaubwürdigkeitsbestimmungen, zu täuschen, indem der Angreifer sein Verhalten anpasst. Dies kann ein Angreifer erreichen, wenn er austestet, welche Aktionen ihm Reputationen einbringen oder zur Identifikation von Spam führen. Gegebenenfalls sind diese Verfahren auch öffentlich zugänglich und die Funktionsweise ist dem Angreifer bekannt. Der Angriff wird dann auf der sozialen Netzwerkebene ausgeführt, betrifft aber die Verfahren auf Anwendungsebene. Diese Art von Angriffen können von einem Angreifer oder einer Gruppe von Angreifern durchgeführt werden. Ein einzelner Angreifer muss über eigens durchgeführte Aktionen versuchen die Verfahren zu täuschen, was zum einen unwahrscheinlich erscheint, da die Verfahren Informationen von mehre-

ren Personen berücksichtigen. Zum anderen können die Teilnehmer solche Angriffe wahrnehmen, wenn ein Teilnehmer viele sichtbaren Aktionen durchführt, die nicht plausibel erscheinen. Eine weitere Möglichkeit für den Angreifer kann es sein, Aktionen von anderen nachzuahmen, wenn diese eine hohe Reputation versprechen. Eine agierende Gruppe dagegen ist schwer zu erkennen und kann sich gegenseitig zu Reputation verhelfen. Ein Vorteil hierbei kann sein, dass eine Gruppe erst eine gewisse Größe erreichen muss, um einige Täuschungen effektiv durchführen zu können. Letztendlich bleibt es die Aufgabe der Verfahren die Erkennungsmuster so zu gestalten, dass diese Angriffe erschwert oder verhindert werden.

Die Angriffe die das Identitätsmanagement von sozialen Netzwerken ausnutzen, stellen auch eine Gefahr für die Authentizität dar und widersprechen dem letzten Punkt in der Auflistung. Angriffe dieser Art zu verhindern, ist Aufgabe des Identitätsmanagement, was allerdings zur Verletzung der Kriterien der Privatsphäre führen kann. Für die weitere Behandlung der Thematik werden auch das Blocken und Filtern von Nachrichten betrachtet, da hierbei nicht nur die Verfügbarkeit, sondern auch die Verbindlichkeit und Integrität betroffen sein können. Vernachlässigt werden dafür Angriffe, die vorrangig die Privatsphäre betreffen.

3.3.5 Soziale Netzwerkebene

Auf der sozialen Netzwerkebene gehen die Angriffe von den Teilnehmern des Netzwerkes aus, welche über ein Profil in dem sozialen Netzwerk verfügen können. Die wichtigsten Angriffe hierbei stammen aus dem Social Engineering, um sensible Informationen zu erhalten oder einen Teilnehmer zur Durchführung bestimmter Aktionen zu bringen. Ein weiterer Angriff kann das Angeben falscher Informationen sein, um andere Teilnehmer zu täuschen. Dieser kann auch mit dem Identitätsmanagement aus dem vorherigen Abschnitt verknüpft werden, wenn mit einer Identität auch weiterer Merkmale (Alter, Geschlecht, E-Mailadresse oder Zahlungsmittel) verbunden sind. Ein anderer Aspekt, der auch eine Gefahr für soziale Netzwerke darstellt, ist das Versenden von Spam. Gibt es keine Sicherheitsmaßnahmen gegen Spam, kann dies auch zu einer starken Störung der User Experience führen, was zur Folge haben kann, dass die Teilnehmer das soziale Netzwerk nicht mehr nutzen. Wird der Spamanteil so hoch, dass sich für die normale Nutzung des Netzwerkes erheblich Verzögerungen ergeben, kann dies auch als ein Angriff auf die Verfügbarkeit interpretiert werden. Cutillo et al. nennen für Angriffe auf der sozialen Netzwerkebene noch Diffamierung und *Ballot Stuffing* als zwei weitere mögliche Angriffe. Der erste Angriff bezeichnet

das Beschädigen des Rufes eines Teilnehmers (in Form eines Unternehmens oder einer natürlichen Person). Dadurch kann es zum Ausschluss des Teilnehmers aus Gruppen oder zu Desinteresse anderer Teilnehmer gegenüber dem angegriffenen Teilnehmer kommen. Beim Ballot Stuffing wird versucht, die Aufmerksamkeit auf einen Teilnehmer zu lenken, so dass ein Interesse von vielen Teilnehmern entsteht. Hieraus kann ein erhöhtes Aufkommen an privaten Nachrichten oder Zugriffen auf das Profil des Teilnehmers resultieren, was wiederrum zu einem Denial-of-Service (DoS) oder einer starken Beanspruchung der Ressourcen des Teilnehmers führen kann.

3.3.6 Diskussion der Angriffe auf sozialer Netzwerkebene

Ein großer Teil der Angriffe, welche auf der sozialen Netzwerkebene ausgeführt wurden, allerdings auf der Anwendungsebene wirken oder Mechanismen auf dieser Ebene aushebeln, wurden schon im vorherigen Abschnitt beschrieben. Somit bleiben hier Angriffe, die unspezifisch hinsichtlich der Anwendungsebene sind und meist die Integrität und Authentizität der Teilnehmerdaten nicht direkt beeinflussen, sondern in bestimmten Fällen dabei helfen, diese Angriffe durchzuführen, wie etwa Social Engineering.

3.4 Zusammenfassung

In diesem Kapitel wurde die Situation für den Rahmen dieser Arbeit und mögliche Angriffe beschrieben. Dafür wurden zuerst die Anreize und Interessen beschrieben, welche je nach sozial-politischer Situation noch weitere Variationen und Prioritäten mit sich bringen. Danach wurden die Angriffe aufgeführt, wobei diese erst allgemein auf den drei Ebenen nach dem Modell von Cutillo et al. ermittelt wurden. Im Anschluss wurde die Relevanz der Angriffe für diese Arbeit diskutiert. Es zeigt sich hierbei, dass die meisten Angriffe, die die Integrität und Authentizität der Teilnehmerdaten betreffen, auf der Anwendungsebene ansetzen. Auf der sozialen Netzwerk- sowie Transport- und Kommunikationsebene lassen sich dagegen zwei wichtige Angriffe nennen, die nicht vernachlässigt werden sollten. Das Verändern von Paketen und Falschangaben. Da allerdings von der Anwendungsebene die meiste Gefahr ausgeht, erscheint es als sinnvoll, den Fokus der weiteren Betrachtungen auf diese Ebene zu legen. Dabei ist ein wichtiger Aspekt, dass zu diesem Zeitpunkt noch keine Aussage zu den spezifischen Angriffen, die sich je nach technischer Umsetzung bzw. Infrastruktur des sozialen Netzwerkes ergeben, getroffen werden kann. Ein weiterer Punkt, den es nach dieser Analyse zu klären gilt, ist die Frage, welche Art von Teil-

nehmerdaten Kriterien besitzen, die bei Manipulationen zu erfüllen sind, damit die Echtheit der repräsentierten Information bestehen bleibt. Um dies zu ermitteln, werden die Daten aus den sozialen Netzwerken hinsichtlich solcher Kriterien im nächsten Kapitel untersucht.

4 Teilnehmerdaten

Nachdem nun ein Überblick zu den Angriffen in sozialen Netzwerken gegeben wurde, soll in diesem Kapitel geklärt werden, wie sich Teilnehmerdaten aus sozialen Netzwerken zusammensetzen und welche Kriterien es gibt, um sie auf Authentizität zu überprüfen. Um dies zu erreichen, werden Arbeiten aus verschiedenen wissenschaftlichen Disziplinen vorgestellt, die Daten aus sozialen Netzwerken verwenden oder die bereits Klassifikationen zu Teilnehmerdaten durchgeführt haben. Damit ein besseres Verständnis für diese Verfahren möglich ist, werden vorher die einzelnen Schritte des Data Mining-Prozesses in sozialen Netzwerken erläutert. Im Anschluss dieser Analyse wird eine eigene Klassifikation von Teilnehmerdaten zur Betrachtung der Authentizität der Daten gegeben und zum Abschluss des Kapitels diskutiert.

4.1 Der Data Mining-Prozess in sozialen Netzwerken

Der Data Mining-Prozess besteht aus mehreren Tätigkeiten, wie dem Selektieren, Aufbereiten, Auswerten und Evaluieren der Daten, wobei zusätzlich für Data Mining in sozialen Netzwerken die Daten noch erhoben werden müssen, wenn kein Zugriff auf die Datenbanken der Dienstanbieter besteht. Das Erheben der Daten kann über Suchanfragen oder durch das direkte Aufrufen von Profilen und dem Herauslesen der Daten von der Weboberfläche des sozialen Netzwerkes getätigt werden. Dabei kann allerdings meist nur ein Teil der Informationen der Teilnehmer aufgrund von Zugriffsbeschränkungen erhoben werden. Des Weiteren kann nur die Art an Daten erhoben werden, die in dem sozialen Netzwerk öffentlich sichtbar sind. Nicht sichtbare Informationen, wie beispielsweise mit welcher Häufigkeit ein Teilnehmer auf eine Profilseite zugreift, können mit dieser Methode nicht erfasst werden. Eine andere Möglichkeit ist es, die APIs der jeweiligen Plattformen zu verwenden, um automatisiert Daten in maschinenlesbarer Form zu beziehen. Insbesondere Twitter bietet sich hierbei für eine Reihe von Studien an, da die Beiträge häufig öffentlich zur Verfügung stehen und mittels der Twitter Streaming API über einen Zeitraum in Echtzeit abgerufen werden können.[12] Hierbei müssen nicht zwangsläufig mehr Daten erfasst werden, als bei den Abfragen über die Weboberfläche, dafür bietet es die Möglichkeit, Informationen über einen bestimmten Zeitraum zu beziehen. Für einige Forschungsarbeiten, wie Verhaltensstudien, kann es notwendig sein, jede Information und Aktion eines Teilnehmers zu erfassen, weshalb hier *Clickstream-Daten*[13]

[12] Eine Hürde die dabei geben ist, ist die Begrenzung der Anfragen für ein Zeitinterval.
[13] Hierbei werden alle Aktionen, sprich jeder Klick usw. des Anwenders aufzeichnet

verwendet werden [8, 55]. Dabei können spezielle Anwendungen oder Dienste verwendet werden, welche alle Aktionen des Nutzers aufzeichnen und gegebenenfalls den Zugriff über mehr als eine Plattform ermöglichen, was den Forschern erlaubt, die Daten von verschiedenen sozialen Netzwerken zu erheben. Alternativ dazu kann auch der Datenverkehr der Teilnehmer zu den sozialen Netzwerken mitgeschnitten und danach ausgewertet werden, wenn ein Zugriff auf den Datentransfer von den ISP zur Verfügung steht.

Nachdem die Daten erhoben wurden, gilt es diese Rohdaten so zu modifizieren, dass sie für den Data Mining-Prozess verwertbar sind. Dies kann das Bereinigen von Inkonsistenz sein, aber auch eine Auswahl von Datensätzen, welche für die Kriterien des Anwendungszwecks oder der Forschungsarbeit relevant sind. Beispielweise kann dies bei Forschungsarbeiten für die Bestimmung der Glaubwürdigkeit von Beiträgen mit Nachrichteninhalten, die Selektion von Beiträgen sein, welche sich einem aktuellen Thema in den Medien widmen. Da es sich allerdings bei den erhobenen Daten meist um eine große Anzahl handelt, kann es viel Zeit in Anspruch nehmen, die Daten selbst auszuwerten beziehungsweise Selektionen durchzuführen. Eine mögliche Lösung hierzu bieten Dienste wie *Amazon mechanical turk*[14], wobei viele Arbeiter eine Reihe von Aufgaben ausführen, zu denen eine Maschine nicht (oder noch nicht) in der Lage ist, wie beispielsweise die Glaubwürdigkeit eines Beitrages eines Teilnehmers bewerten.

Nach der Auswahl der Datensätze müssen Attribute definiert und gegebenenfalls diskretisiert werden, die für das anschließende Data Mining relevant sind. Bei Glaubwürdigkeitsanalysen in sozialen Netzwerken werden beim Data Mining häufig Klassifikationsansätze verwendet. Hierbei sollen Zusammenhänge in einer Datenmenge erkannt werden, die beispielsweise in einer Funktion oder einem Entscheidungsbaum resultieren, um Objekten Klassen zuzuordnen. Für Glaubwürdigkeitsanalysen können die vordefinierten Klassen beispielsweise ein glaubwürdiger Beitrag, ein unglaubwürdiger Beitrag oder nicht einordbarer Beitrag sein. Entscheidend für die Qualität der Erkennung sind neben den Daten die vorher definierten Attribute. Bei Glaubwürdigkeitsanalysen ist ein häufig verwendetes Attribut die Anzahl der Retweets eines Beitrages, um diesen als Glaubwürdigkeitsindikator für Beiträge heranzuziehen. Werden dazu noch weitere Attribute definiert, wie die durchschnittliche Anzahl der Retweets der Beiträge eines Teilnehmers, so kann eine höhere Aussagekraft über die Glaubwürdigkeit eines Beitrags erreicht werden, als vergleichsweise durch die Verwendung von nur einem Attribut. Die Wahl der richtigen Attribute ist also ein

[14] https://www.mturk.com/mturk/, letzte Sichtung 30.11.2013

entscheidender Faktor für die Qualität der Ergebnisse. Des Weiteren können die Attribute für den jeweiligen Kontext eine verschiedene Aussagekraft besitzen. Nachdem der Data Mining-Prozess ein entsprechendes Model in einer Trainingsphase erstellt hat, können auch größere Datenmengen ausgewertet werden. Am Ende des Data Mining-Prozeses erfolgt die Evaluation und Interpretation der Ergebnisse, hinsichtlich der Qualität der Ergebnisse, Überprüfung der aufgestellten Hypothesen oder auch der verwendeten Attribute.

4.2 Merkmale von Teilnehmerdaten

Nachdem die Basis durch die Diskussion der Anwendungsfälle von authentischen Teilnehmerdaten und durch den Einblick in die Funktionsweise von Data Mining für dieses Kapitel geschaffen wurde, gilt es nun zu ermitteln, welche Merkmale von Teilnehmerdaten es in sozialen Netzwerken geben kann. Hierfür werden nun einige Verfahren vorgestellt, die aus dem Bereich der Spamerkennung, Glaubwürdigkeitsbestimmung und Verhaltensforschung stammen. Des Weiteren werden allgemeine Taxonomien von Teilnehmerdaten in sozialen Netzwerken angeführt. Die Behandlung von Arbeiten aus verschiedenen Forschungsbereichen bringt den Vorteil gegenüber der reinen Betrachtung von Daten, die von den Providern der sozialen Netzwerke erhoben werden, dass die Teilnehmerdaten aus unterschiedlichen Perspektiven betrachtet werden und somit eine breitere Analyse ermöglichen. Des Weiteren können so verschiedene Verwendungszwecke erfasst werden. Innerhalb dieses Abschnittes wird nicht explizit auf die Daten, die von den Anbietern sozialer Netzwerken, wie [37] erfasst werden, eingegangen. Sie sind allerdings auch bei der Entwicklung der eigenen Klassifikation mit eingeflossen.

4.2.1 Teilnehmerdaten für die Glaubwürdigkeitsbestimmung

Die Merkmale in diesem Abschnitt bestehen aus den Attributen der Data Mining-Verfahren, die innerhalb einiger Forschungsarbeiten im Bereich der Glaubwürdigkeitsanalysen von Tweets in Twitter und der Erkennung von Spammern in sozialen Netzwerken entstanden sind. Dabei ist anzumerken, dass die Attribute und Klassifikationen, die sich auf eine Plattform beziehen, kein Hindernis für eine allgemeine Betrachtung darstellen, da sie sich zum größten Teil auf andere Plattformen adaptieren oder generalisieren lassen.

Verfahren zur Glaubwürdigkeitsbestimmung in Twitter Die Arbeit von Cutillo et al. [15] untersucht, ob die Glaubwürdigkeit von Inhalten in der Plattform Twitter automatisch ermittelt werden kann. Hierfür soll zum einen automatisch erkannt werden, ob es sich bei einem Tweet um eine News oder einen Chat handelt. Ein Chat ist dabei eine Konversation oder eine subjektive Meinungsäußerung und eine News eine berichtenswerte Aussage, welche einen Fakt oder eine Information bezeichnet, die auch für Personen außerhalb des Freundeskreises des Autors eine Relevanz besitzt. Zum anderen werden die Tweets der Kategorie News thematisch anhand von Schlüsselwörtern[15] gruppiert. Um danach einen Klassifizierer für die Bestimmung der Glaubwürdigkeit eines Tweets bzw. Themas für den Data Mining-Prozess zu trainieren, verwenden die Autoren unterschiedliche Kategorien von Attributen, welche in *Message-*, *User-*, *Topic-* und *Propagation-based Features* unterteilt werden.

- **Message-based Features** beziehen sich auf die Merkmale des Inhaltes sowie die Eigenschaften eines Tweets, wie Satzeichen, Länge des Tweets, der Wochentag, ob es ein Retweet ist und so weiter.
- Die Attribute der **User-based Features** beziehen sich auf die Eigenschaften des Autors der Nachricht und sein soziales Netzwerk, wie das Registrierungsjahr, Status der Verifizierung, Anzahl der abonnierten Teilnehmer und Follower sowie die Anzahl der Tweets.
- Die Kategorie **Topic-based Features** fassen die Attribute aus den vorherigen beiden Kategorien pro Thema zusammen und summieren diese gegebenenfalls auf. Hierzu gehört unter anderem die Fraktion der Tweets mit einer URL, die Anzahl verschiedener URLs, das durchschnittliche Alter der Teilnehmer und die Anzahl verschiedener Hash-Tags.
- Die letzte Kategorie **Propagation-based Features** bezieht sich auf die Retweets eines Tweets, wie die Tiefe eines Retweetbaumes.

Aufbauend auf den Erkenntnissen von Castillo et al., verfolgen Gupta et al. [34] mit ihrem Verfahren das Ziel, die Glaubwürdigkeit von Twitter-Events[16] zu bestimmen. Ein Event ist hierbei eine Menge von Tweets, wobei die Tweets eine Reihe von Schlüsselwörter beinhalten, die spezifisch für das Event sind. Die Autoren berücksichtigen in ihrem Verfahren, die Beziehungen zwischen den Entitäten, wie Tweets,

[15] Beispielsweise können die Schlüsselwörter *„Obama"*, *„Romney"* und *„election"* verwendet werden, um einen Beitrag zu dem Thema Wahlen in den Vereinigten Staaten zu zuordnen.

[16] Dies ist ein Synonym für die Bezeichnung *Themen* bei Castillo et al.

Events und Teilnehmern und versuchen diese Abhängigkeiten für die Glaubwürdigkeitsbestimmung zu nutzen, da beispielsweise ein glaubwürdiger Teilnehmer auch mit höherer Wahrscheinlichkeit einen glaubwürdigen Tweet verfasst. Diese Beziehungen zwischen den Entitäten werden mit Hilfe von Graphen modelliert und erlauben es, Glaubwürdigkeitsbewertungen der Entitäten zu aggregieren. Um die Bewertungen zu aggregieren, müssen vorher allerdings Glaubwürdigkeitsbewertungen für die einzelnen Entitäten durchgeführt werden, weshalb die Autoren einen Klassifizierer verwenden, welcher ähnliche Kategorien (*User*, *Tweet* und *Event Features*) wie bei Castillo et al. mit ein paar Modifikationen bei den Ausprägungen verwendet. Die User Features beziehen sich auf die Vollständigkeit des Profils eines Teilnehmers und zeigen somit keine Abweichungen zu User-based Features. Auch Tweet- und Eventattribute haben im Vergleich zu Castillo et al. kaum Unterschiede, bis auf die Attribute, bei denen auch Aussagen qualitativ bewertet werden, ob ein Tweet seriös ist, ob er in der ersten, zweiten oder dritten Person verfasst wurde oder ob die Aussage mit der allgemeinen Aussage des Themas übereinstimmt. Des Weiteren werden bei event features auch zeitliche Aspekte berücksichtigt, wie welche Anzahl an Tweets zu einem Event zum Zeitpunkt der höchsten Popularität veröffentlich werden oder wie viele Stunden ein Event populär ist. Die Beziehungen zwischen den Tweets werden zwar nicht für den Klassifizierer verwendet, sind aber auch ein relevantes Merkmal für Teilnehmerdaten in sozialen Netzwerken.

Eine weitere Arbeit in diesem Bereich stammt von Kang et al. [43], welche drei verschiedene Modelle für die Bestimmung der Glaubwürdigkeit von themenspezifischen Informationen evaluiert. Jedes Modell verwendet dabei eine andere Kombination von Attributen. Für das *Content Model* werden nur Attribute verwendet, welche sich auf die Inhalte einer Nachricht beziehen, wie schon die Tweet bzw. Message-based Features in den Verfahren der beiden Vorgänger. Das *Social Model* beinhaltet Attribute, die das soziale Netzwerk betreffen, beispielsweise die Anzahl der Retweets eines Teilnehmers im Verhältnis zu der Anzahl der Retweets in einem Themenbereich oder wie häufig ein Teilnehmer mit anderen Teilnehmern, die über ein Thema schreiben, verbunden ist. Für das *Hybrid Model* stellen die Autoren mehrere verschiedene Kombinationen auf, dabei handelt es sich jedoch um Zusammensetzungen der Attribute aus dem Content Model und dem Social Model.

4.2.2 Merkmale für Spamerkennung

Ein weiteres Anwendungsgebiet, welches auch in anderen Bereichen Aufmerksamkeit erhält, ist das Unterbinden von Spam-Nachrichten. Die Arbeit von Benevenuto et al. [7] behandelt die Erkennung von Spammern und Spam-Nachrichten in Twitter mittels maschinellen Lernens. Für den Klassifizierer haben die Autoren die Attribute in zwei Kategorien unterteilt. Zum einen in *Content Attributes*, womit Attribute gemeint sind, die wie im vorherigen Abschnitt, Merkmale des Textes eines Tweets erfassen und zum anderen *User Behaviour Attributes*, welche sich auf das Verhalten und das soziale Netz eines Teilnehmers beziehen. Die Besonderheit der Content Attributes ist, dass die Wörter eines Tweets mit einem Katalog von bekannten Wörtern für Spam abgeglichen werden. Teilnehmerverhaltensattribute weichen mit wenigen Übereinstimmungen von den vorherigen Arbeiten ab und beinhalten Attribute wie die Anzahl der Tweets eines Nutzers, wie oft der Teilnehmer erwähnt wird und das Verhältnis von Follower zu Followees. Somit kann das Verhalten eines Teilnehmers und wie das soziale Netzwerk auf ihn reagiert, erfasst werden.

Stringhini et al. [59] versuchen in ihrer Arbeit, Spammer in mehreren sozialen Netzwerken automatisch zu erkennen. Dafür beobachten die Autoren Aktivitäten von anderen Teilnehmern, insbesondere Spammern, mit Hilfe von *Honey Pots*. Als Honey Pots sind in diesem Fall Accounts bei verschiedenen sozialen Netzwerken zu verstehen, welche die Aktionen anderer Teilnehmer, wie Freundschaftsanfragen, private Nachrichten und Pinnwandeinträge protokollieren. Um aus der gewonnenen Datenmenge Spammer erkennen zu können, setzen die Autoren ebenso auf maschinelles Lernen, wofür sie sechs Attribute verwenden. Zu diesen sechs Attributen zählen die Anzahl der Freunde, die Anzahl verfasster Nachrichten, die Anzahl der Nachrichten mit einer URL, der Grad der Übereinstimmung der Nachrichten, die Anzahl der Freundesanfragen, die ein Teilnehmer versendet, im Verhältnis zu der Gesamtanzahl aller Freunde und die Anzahl verschiedener Profilnamen im Verhältnis zu allen Profilnamen der Freunde eines Teilnehmers. Eine Übersicht der Kategorien der bis hierhin vorgestellten Verfahren und ein paar Beispielmerkmalen ist in Abbildung 3 dargestellt.

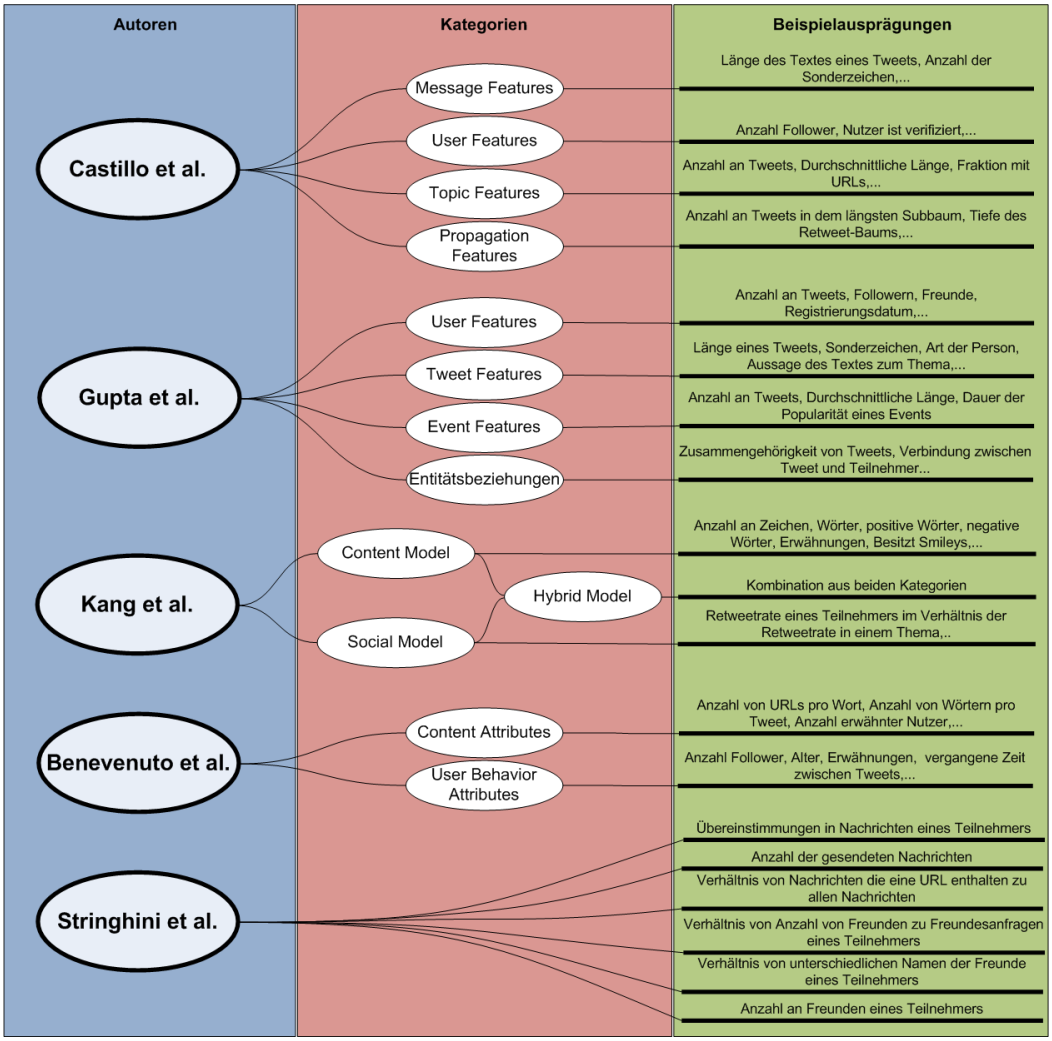

Abbildung 3: Grafischer Überblick der Klassifizierungen von Castillo, Benevenuto, Kang und Gupta et al.

4.2.3 Verhaltensstudien mit Clickstream-Daten

Ein weiterer Forschungsbereich im Zusammenhang mit sozialen Netzwerken ist der von Verhaltensstudien, welche die Aktivitäten der Teilnehmer analysieren. Daraus lässt sich erschließen, welche Funktionen des sozialen Netzwerkes häufig verwendet werden, da diese Aufschluss über wichtige Funktionen und das verursachte Datenvolumen geben. Diese Informationen können dafür verwendet werden, die Auswahl und Gestaltung von Funktionen und das Design der Infrastruktur eines sozialen Netzwerkes oder des darunterliegenden Netzes zu beeinflussen. Benevenuto et al. [8] und

Schneider et al. [55] verwenden hierfür in ihren Arbeiten jeweils Clickstream-Daten, um möglichst alle Aktionen der Teilnehmer erfassen zu können. Im Vergleich zu den vorherigen Verfahren, werden dabei keine Merkmale und deren Ausprägungen betrachtet, sondern der Fokus auf die Art der Aktion der Nutzer gelegt. Eine Aktion kann beispielsweise der Aufruf eines Profils, das Verfassen einer Nachricht oder Interagieren mit einer Anwendung sein. Die Kategorisierung dieser Aktionen von Benevenuto et al. ist in Tabelle 5 dargestellt, wobei ein Scrapbook alle Textnachrichten darstellt, die ein Teilnehmer erhalten hat und ein Testimonials Kommentare von anderen Teilnehmern zu einem Teilnehmer sind. Darüber hinaus sind die Metadaten einer Aktion weiterer Merkmale, die erfasst werden. Hierzu gehören der Zeitpunkt und die geografische Position des Teilnehmers bei der Durchführung der Aktion. Des Weiteren wird erfasst, wie lange ein Teilnehmer sich in dem sozialen Netzwerk aufhält (auch Sitzung genannt), über welche Art von Gerät der Teilnehmer sich einloggt und ob mehrere Sitzungen gleichzeitig stattfinden, beispielsweise durch die Verwendung mehrerer Geräte.

4.2.4 Taxonomien für soziale Netzwerkdaten

Während in den vorherigen Abschnitten Einordnungen von Teilnehmerdaten vorgestellt wurden, die zur Bearbeitung der Problemstellungen aus den jeweiligen Forschungsarbeiten entstanden sind, widmen sich die Taxonomien in diesem Abschnitt der generellen Einordnung von Daten in sozialen Netzwerken. Innerhalb dieses Abschnittes werden die Taxonomien von Schneier [56] und Cutillo et al. [19] vorgestellt. Eine Übersicht zu den beiden Taxonomien ist in Abbildung 4 dargestellt.

In der Taxonomie von Schneier werden Teilnehmerdaten in sechs Kategorien unterteilt:

1. **Service data** - Hiermit sind Daten gemeint, die ein Nutzer an den Anbieter des Netzwerkes gibt, um das soziale Netzwerk zu nutzen. Dies können Beispielsweise der Name, die E-Mailadresse, das Geburtsdatum oder Zahlungsinformationen sein.

2. **Disclosed data** - Diese Kategorie umfasst Daten, die ein Teilnehmer über seine Seite in dem sozialen Netzwerk veröffentlicht. Dies können Kommentare, Fotos, Nachrichten, Videos, Verlinkungen und so weiter sein.

3. **Entrusted data** - Hier drunter fallen die gleichen Daten wie in der Kategorie Disclosed Data, mit dem Unterschied, dass der Teilnehmer diese auf der Seite

eines anderen Teilnehmers hinterlässt. Der Teilnehmer gibt dabei einen Teil seiner Kontrolle über die Daten ab, da der andere Teilnehmer diese möglicherweise löschen, editieren oder verbergen kann und die Sichtbarkeit der Daten durch die Präferenzen des anderen Teilnehmers bestimmt werden.

4. **Incidental data** - Incidental-daten beziehen sich auf Aktionen von Dritten, die Informationen über einen Teilnehmer freigeben. Dies kann beispielsweise ein Beitrag eines Teilnehmers über einen anderen Teilnehmer oder das veröffentlichen eines Fotos sein. Der Teilnehmer hat dabei meist keinen Einfluss darauf, was die andere Teilnehmer über ihn preisgeben und kann erst nach der Veröffentlichung reagieren, wobei er auch danach nur bedingt Einfluss nehmen kann. Facebook beispielsweise bietet die Möglichkeit, dass ein Teilnehmer erst zustimmen muss, ob eine Verlinkung auf einem Bild zu seinem Profil veröffentlich wird. Somit kann der Teilnehmer verhindern, dass ein Bild direkt mit ihm verbunden wird, trotzdem bleibt das Bild in dem sozialem Netzwerk bestehen und es ist möglich, dass der Anbieter weiterhin die Information speichert, dass sich der Teilnehmer auf dem Bild befindet oder eine Assoziation mit ihm besteht.

5. **Behavioral data** - Hiermit sind Daten gemeint, die das Verhalten des Teilnehmers protokollieren. Dabei handelt es sich um die Aktivitäten eines Teilnehmers, wie schon im Abschnitt 4.2.3 beschrieben. Des Weiteren gehören dazu auch Daten, welche Informationen der Teilnehmer nutzt, wie beispielsweise welche Verlinkungen der Teilnehmer aus dem sozialen Netzwerk heraus aufruft und welche Informationen sich daraus ableiten lassen.

6. **Derived data** - Unter diese Kategorie fallen Daten, die sich mittels der Daten aus den vorherigen Kategorien extrahieren lassen. Hierfür können Methoden wie beispielsweise das Data-Mining zum Einsatz kommen.

Eine zweite Taxonomie für Teilnehmerdaten stammt von Cutillo et al. [19] und beinhaltet die fünf folgenden Kategorien:

1. **Personal contact details** - Dieser Punkt beinhaltet Informationen, die das Profil des Teilnehmers umfassen, wie eine kurze Beschreibung, Name, Foto, Kontaktinformationen, Wünsche und Vorlieben. Hinzu kommen Metainformationen, wie der Registrierungszeitpunkt.

2. **Connectivity** - Darunter fallen die sozialen Kontakte eines Teilnehmers und Informationen über die Verbindungen, die der Teilnehmer mit dem jeweiligen

Kontakt hat. Zusätzlich können hierzu Empfehlungen zu anderen Teilnehmern kommen.

3. **Interests of the user** - Dies beschreibt Interessen, Vorlieben, Einstellungen und freizeitliche Aktivitäten oder auch Gruppenzugehörigkeiten.

4. **Information on the curriculum vitae** - Hiermit sind schulische, akademische und berufliche Erfahrungen sowie Auszeichnungen gemeint. Des Weiteren können darunter Mitgliedschaften in Organisationen oder Positionen in Klubs gehören.

5. **Communication -** Diese Kategorie umfasst die Kommunikation eines Teilnehmers mit anderen Teilnehmern, wie das Verfassen von Nachrichten, Pinnwandeinträge und so weiter. Hinzu können noch weitere Möglichkeiten kommen, welche abhängig von der entsprechenden Plattform sind, wie das Anstupsen oder Erwähnen eines Teilnehmers.

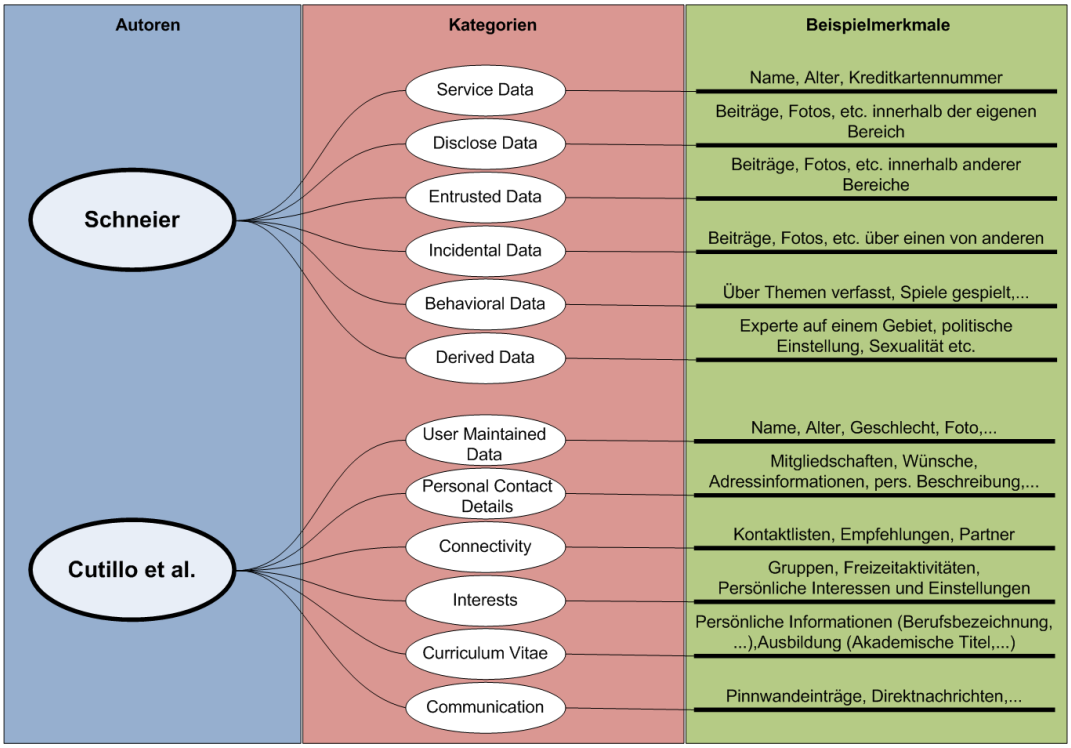

Abbildung 4: Grafischer Überblick der Klassifizierungen von Cutillo et al. und Schneier zu sozialen Netzwerkdaten

4.3 Klassifikation für die Authentizität von Teilnehmerdaten

Da nun ein Überblick für mögliche Merkmale von Teilnehmerdaten in sozialen Netzwerken geschaffen wurde, wird in diesem Abschnitt eine Klassifikation für Teilnehmerdaten nach charakteristischen Merkmalen zur Erfüllung der Authentizität vorgestellt. Des Weiteren wird diskutiert, was mögliche charakteristische Merkmale für Teilnehmerdaten sind. Ein Überblick der Klassifikation ist in Abbildung 5 dargestellt.

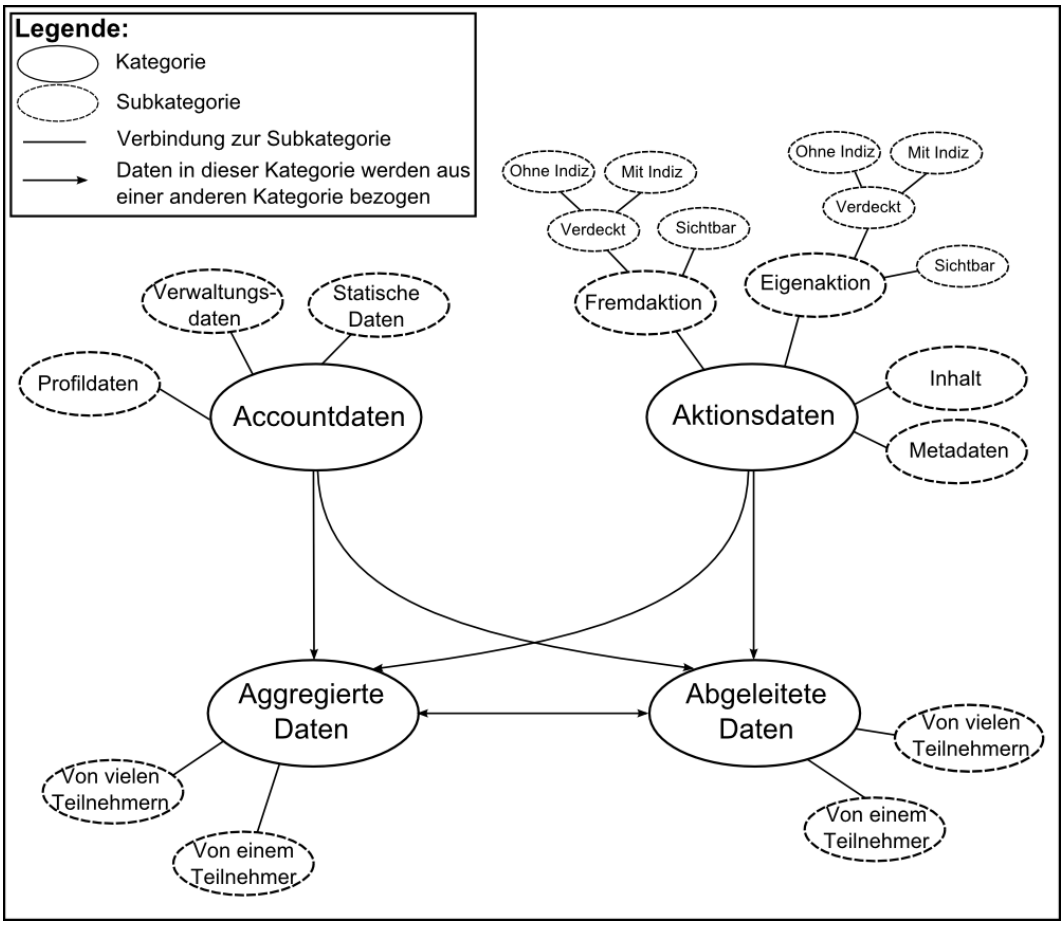

Abbildung 5: Überblick der eigenen Kategorisierung von Teilnehmerdaten in sozialen Netzwerken

4.3.1 Accountdaten

Die erste Kategorie innerhalb dieser Klassifizierung kann in drei Subkategorien unterteilt werden (siehe auch Tabelle 2) und umfasst alle Daten, die für den Account

und das Profil eines Teilnehmers relevant sind. Die erste Subkategorie, welche hier als Profildaten bezeichnet wird, beinhaltet alle Daten, die zu dem Profil eines Teilnehmers gehören, ähnlich wie bei Cutillo et al. die Kategorie personal contact details. Dabei kann es sich für die anderen Teilnehmer sowohl um sichtbare als auch nicht sichtbare Informationen handeln, wobei die Sichtbarkeit der Information je nach Plattform und Einstellungen der Teilnehmer variieren kann. Als Beispiel kann die Information über das Alter eines Teilnehmers herangezogen werden. In einer Plattform, wie beispielsweise einer Singlebörse, ist dies möglicherweise ein entscheidendes Kriterium, um mit jemanden in Kontakt zu treten, während es in anderen sozialen Netzwerken möglich ist, diese Information auszublenden. Die zweite Subkategorie ist ähnlich zu der Kategorie *Service Data* von Schneier und umfasst die Daten, die ein soziales Netzwerk für die Umsetzung bestimmter Funktionen benötigt, wie die Kreditkartennummer zur Durchführung von Zahlungen oder eine E-Mailadresse zur eindeutigen Identifizierung oder Benachrichtigung eines Teilnehmers. Diese Daten haben möglicherweise keine Bedeutung für andere Teilnehmer des sozialen Netzwerkes und sind für diese nicht sichtbar, da es sich hierbei meist um sensible Daten handelt. Für den weiteren Verlauf wird diese Subkategorie als Verwaltungsdaten bezeichnet. Die letzte Subkategorie, umfasst statische Daten für einen Account, die im Gegensatz zu den zwei vorherigen Subkategorien nicht von dem Teilnehmer selbst verwaltet, sondern durch das System erstellt werden, wie das Registrierungsdatum oder eine eindeutige Bezeichnung für einen Account.

Die drei Subkategorien lassen sich auf unterschiedliche Arten auf Authentizität bzw. Echtheit überprüfen. Bei den Verwaltungsdaten kann dies mittels Kontrollen umgesetzt werden. Das kann bedeuten, dass beispielsweise der Teilnehmer zur Überprüfung seiner E-Mailadresse eine Bestätigungsemail erhält, welche Informationen beinhaltet, mit denen der Teilnehmer bestätigen kann, dass er Zugriff auf die E-Mailadresse hat. Eine anderer Anwendungsfall ist die Überweisung eines geringen Geldbetrages auf ein Bankkonto, wobei der Verwendungszweck innerhalb der Überweisung eine Informationen zur Bestätigung des Kontos beinhaltet.

Profildaten, wie das Alter, der Wohnort oder eine Mitgliedschaft lassen sich Beispielsweise mittels Komponenten des Identitätsmanagements überprüfen, welche eine Identitätsüberprüfung beinhalten kann, indem der Nutzer eine Kopie seines Personalausweises oder anderer Zeugnisse an eine vertrauenswürdige Instanz schickt. Diese Methode lässt sich auch für einen Teil der Verwaltungsdaten einsetzen, wenn Informationen wie das Geburtsdatum und der reale Name wesentlicher Faktor darstellen. Die Durchführung dieser Methode wird allerdings gegebenenfalls

sehr aufwendig, wenn ein Nutzer häufig seine Angaben wechselt, er viele Angaben belegen muss, er keine Belege für die Angaben besitzt und wenn ein soziales Netzwerk verwendet wird, in dem keine zentrale Organisationseinheit existiert. Des Weiteren lassen sich einige andere Informationen in dem Profil, wie die persönliche Beschreibung, nur schwer auf Echtheit überprüfen. Es besteht zwar die Möglichkeit, die Informationen mittels der Zustimmung anderer Teilnehmer des sozialen Netzwerkes zu überprüfen, dies gibt allerdings keine hinreichende Sicherheit, denn eine Beschreibung, die ein Teilnehmer über sich selbst abgibt, weicht möglicherweise von der Wahrnehmung anderer Teilnehmer ab. Nichtsdestotrotz lässt sich die Urheberschaft für Profil- und Verwaltungsdaten als Kriterium für die Authentizität heranziehen.

Bei der dritten Subkategorie, den statischen Daten, ist zu beachten, dass sich die Daten dieser Kategorie nicht mehr ändern lassen. Das heißt die Daten sind authentisch, wenn sie seit der Erstellung des Accounts nicht mehr geändert wurden, korrekte Information angegeben sind und eindeutig einem Account zugeordnet werden können.

4.3.2 Aktionsdaten

Während die vorherige Kategorie Daten umfasst, die für das Profil und den Account des Teilnehmers relevant sind, werden in dieser Kategorie Daten erfasst, die mit den Aktionen eines Teilnehmers oder den Interaktionen mit anderen Teilnehmern des sozialen Netzwerkes verbunden sind (siehe auch Tabelle 3). Eine Interaktion kann andere Teilnehmer, Gruppen oder nur den ausführenden Teilnehmer betreffen. Eine Reihe von möglichen Interaktionen werden durch die Clickstreamdaten aus Abschnitt 4.2.3 aufgezeigt, wobei Abbildung 5 einen Überblick der Aktionen gibt. Dabei kann, wie von Benevenuto et al. [8] angemerkt, zwischen versteckten und sichtbaren Aktionen unterschieden werden. Eine versteckte Aktion kann beispielsweise das Aufrufen eines Profils eines anderen Teilnehmers oder des eigenen Profils sein. In einigen sozialen Netzwerken ist die Information, wer ein Profil aufgerufen hat, durch den Besitzer eines Accounts unter einer Rubrik wie *letzte Besucher* einsehbar. Bei einigen anderen Plattformen bleibt diese Information jedoch für andere Teilnehmer verborgen. Aus diesem Grund wird an dieser Stelle noch ein weiteres Kriterium eingeführt, nämlich die Existenz von möglichen Indizien für die Durchführung einer Aktion. Ein Indiz kann beispielsweise der Aufruf eines Profils auf einer Plattform mit einer zentralen Organisationseinheit sein, wenn hierbei das Geräte des

Endanwenders eine Anfrage an den Server des Anbieters stellt. Der Datentransfer ist somit das Indiz für die Durchführung der Transaktion. Nimmt man dagegen an, dass die Daten noch im Speicher der Maschine des Anwenders liegen, so kann es sein, dass diese Aktion keine nachweisbaren Indizien hervorruft, da keine Anfrage gestellt werden muss. Dabei ist zu beachten, dass auch jeder Aufruf eines Profils gezählt werden kann, womit sich auch die Aufrufe auf das eigene Profil erfassen ließen, solange das Gerät des Anwenders diese Information an das soziale Netzwerk meldet. Weitere Beispiele für verdeckte Aktionen sind Suchanfragen oder einzelne Interaktionsschritte innerhalb eines Profils, wie das Ansehen eines Bildes, Videos und Profils. Der Unterschied hierbei ist, dass beispielsweise bei dem Abrufen eines eigenen Profils kein anderer Teilnehmer betroffen ist. Dieser Fall wird bei der Betrachtung der sichtbaren Aktionen verdeutlicht. Bei sichtbaren Aktionen handelt es sich um Aktionen, die für mindestens einen anderen Teilnehmern des sozialen Netzwerkes sichtbar sind, wie das Verfassen eines Beitrages oder verfasste Beiträge von anderen auf der eigenen Seite des Teilnehmers. Das Verfassen beziehungsweise Veröffentlichen eines Beitrages auf der eignen Pinnwand hat in sozialen Netzwerken häufig die Auswirkung, dass der Beitrag in dem Newsfeeds der anderen Teilnehmer angezeigt wird, die Neuigkeiten von diesem Teilnehmer abonniert haben. Somit wird die Aktion auch für andere sichtbar. Ebenso kann ein Beitrag eines anderen Teilnehmers auf der eigenen Seite für andere Teilnehmer sichtbar werden, insofern dieser nicht von dem Teilnehmer blockiert wird. Des Weiteren kann eine sichtbare Aktion auch die Veränderung des Profils durch einen Teilnehmer sein, da diese Aktion in einigen sozialen Netzwerken[17] zu einer Benachrichtigung der anderen Teilnehmer führt und an andere Teilnehmer direkt kommuniziert wird. Die Veränderung lässt sich allerdings auch durch das Abrufen der Profilinformationen durch einen berechtigten Teilnehmer beobachten. Somit lässt sich festhalten, dass einige Informationen je nach den Eigenschaften der Plattform für andere Teilnehmer sichtbar oder verdeckt ablaufen und somit gegebenenfalls Indizien für die Existenz der Aktion liefern. Des Weiteren können sich diese Aktionen ausschließlich auf den ausführenden Teilnehmer beziehen, aber auch die Teilnehmerdaten anderer Teilnehmer betreffen, wie das Hinterlassen eines Beitrages auf der Pinnwand eines anderen Teilnehmers. Dabei ist zu beachten, dass die Authentizität einer Aktion eines anderen Teilnehmers, die die eigenen Teilnehmerdaten betreffen, nur gegeben ist, wenn auch nachgewiesen werden kann, dass der andere Teilnehmer diese Aktion durchgeführt hat (Fremdakti-

[17] In dem sozialen Netzwerk Xing werden beispielsweise innerhalb des Newsletters befreundete Teilnehmer informiert, wenn ein Teilnehmer Informationen über sich bearbeitet.

on). Ein Kommentar eines Teilnehmers an der Pinnwand eines anderen Teilnehmers muss also durch einen Nachweis für die Durchführung dieser Aktion des Teilnehmers belegt werden. Sichtbare Aktionen, die ein Teilnehmer durchführt, sind soweit authentisch, wenn geprüft wurde, ob der Teilnehmer berechtigt ist diese Aktionen durchzuführen und wenn belegt werden kann, dass die Aktionen von dem Teilnehmer stammen. Eine Fremdaktion, wie beispielsweise das Hinterlassen eines Beitrages auf der Pinnwand eines anderen Teilnehmers, ist nur zulässig, wenn der Teilnehmer die Berechtigung für diese Aktion besitzt und somit auch erst dann authentisch, da sie andernfalls nicht existieren darf beziehungsweise durgeführt werden kann. Bei verdeckten Aktionen stellt sich die Frage, inwiefern diese authentisch vorliegen müssen und wie sich diese überprüfen lassen, wenn kein anderer Teilnehmer Zugriff auf diese Informationen hat. Auch wenn Informationen nicht sichtbar sind, können diese Anwendung bei den vorher beschriebenen Verfahren finden. Das Attribut aus dem Verfahren von Stringhini et al. misst beispielsweise das Verhältnis zwischen der Anzahl der versendeten Freundesfragen zu der Anzahl der Freunde eines Teilnehmers. Die Anzahl der Freundesanfragen ist dabei für keinen Teilnehmer, außer eventuell für den Dienstanbieter der Plattform, sichtbar. Eine einzelne Anfrage ist wiederrum für den jeweiligen angefragten Teilnehmer sichtbar. Die Aggregation dieser für die Öffentlichkeit versteckten Information kann dabei trotzdem helfen Spammer zu identifizieren, stellt allerdings auch eine mögliche Verletzung der Privatsphäre dar, wenn andere Teilnehmer sehen können, dass ein Teilnehmer von anderen Teilnehmern sozial gemieden wird. Schwierig wird es allerdings, wenn eine Aktion keine Hinweise auf ihre Durchführung zulässt, da die Daten für den Aufruf lokal auf dem Gerät des Teilnehmers liegen. So kann es in einigen Fällen nur möglich sein, diese Aktion zu erhalten, wenn der Teilnehmer die Information über seine Aktivität selbst an das soziale Netzwerk sendet.

Bis hierhin wurde nur betrachtet, welche Arten von Aktionen es gibt und wer davon betroffen ist. Zu einer Aktion gehören allerdings auch Metadaten oder Inhalte einer Aktion. Die Metadaten bestehen dabei aus Daten, wie dem Zeitpunkt sowie von welchem Gerät mit welchem Betriebssystem die Aktion durchgeführt wurde, welche IP-Adresse der Teilnehmer hat und somit auch an welchem Standort der Teilnehmer sich gerade befindet oder welchen Browser beziehungsweise Anwendung und Version der Teilnehmer auf seinem Gerät installiert hat [37]. Diese Daten können zum einen wichtig sein, um Reply-Attacken zu verhindern, da Aktionen, welche zu weit in der Vergangenheit liegen, von anderen Teilnehmern ignoriert werden können. Zum anderen können Informationen über das Gerät Aufschluss darüber geben,

wie man den Teilnehmer in ein Netzwerk einbindet. Da in bestimmten dezentralen Systemen die Teilnehmer auch Aufgaben in dem Netzwerk übernehmen, kann diese Information verwendet werden, um die spezifischen Eigenschaften des Gerätes des jeweiligen Teilnehmers einzugehen. Beispielsweise verfügt ein Teilnehmer, der mittels eines Smartphone an dem Netzwerk partizipiert, meist über weniger Ressourcen als Teilnehmer mit einem Laptop. Die Authentizität dieser Daten lässt sich zum einen damit überprüfen, dass die Urheberschaft gesichert ist und die Daten nicht verändert wurden. Problematisch ist es allerdings diese unverfälscht zu beziehen, da beispielsweise die korrekte IP-Adresse über Proxy-Server verschleiert werden kann. Ebenso lassen sich auch Informationen über das Gerät verschleiern[18] oder die GPS-Koordinaten selbst bestimmen.[19] Des Weiteren lassen sich hieraus auch Verbindungen zwischen den Teilnehmern ableiten, da Beispielsweise protokolliert werden kann, wer sich alles von einem Gerät anmeldet. Dies Art der Informationen gehören aber zu der Kategorie, der aggregierten Daten (siehe Abschnitt 4.3.3).

Die Inhalte einer Aktion sind beispielsweise der Text in einem Beitrag, das Bild oder Video, welches ein Teilnehmer hochladen kann. Die Daten können als authentisch angesehen werden, insofern die Urheberschaft der Aktion geprüft ist und der Inhalt nicht verändert wurde. Allerdings kann der Inhalt an sich auch auf Authentizität überprüft werden. Als Beispiel kann ein Text genommen werden, den der Teilnehmer nicht selbst verfasst hat, sondern von einem anderen Teilnehmer kopiert oder aus einer anderen Quelle entnommen wurde. In diesem Fall ist der Teilnehmer nicht der Urheber des Textes, allerdings lässt es sich, insbesondere wenn der Text aus anderen analogen Quellen stammt, nur mit viel Aufwand prüfen, ob der Teilnehmer der Urheber ist. Stammt der Text aus dem sozialen Netzwerk, so können Überprüfungen auf Übereinstimmungen von Texten mit anderen Teilnehmern vorgenommen werden, um gegen diesen Fall vorzugehen. Eine Motivation für einen Angreifer zum Kopieren von Texten von anderen Teilnehmern könnte es sein, die Reputation, die ein Text erzeugt, für sich selbst zu nutzen. Auf der anderen Seite kann es sich bei dem Text auch um ein Sprichwort oder Redewendung handeln, die von vielen Teilnehmern genutzt wird. Weitere Informationen, die aus den Inhalten einer Aktion gewonnen werden kann, sind beispielsweise die Metainformationen eines Bildes, wie der Ort und das Datum oder auch die Information, die aus einer Aussage abgeleitet werden kann. Diese Daten gehören allerdings in die Kategorie abgeleitete Daten und

[18] Dies kann beispielsweise über das Deaktivieren von JavaScript im Browser oder über die Verwendung von Proxys erreich werden

[19] Es lassen sich beispielsweise durch die Verwendung eines Simluators für mobile Endgeräte die GPS-Koordinaten selbst festlegen.

werden in Abschnitt 4.3.4 weiter besprochen.

4.3.3 Aggregierte Daten

Unter diese Kategorie fallen alle Informationen, die aus mehreren Daten eines oder mehrerer Teilnehmer bestehen (siehe auch Tabelle 4). Die Aggregation von Daten für einen einzelnen Teilnehmer kann beispielsweise die Anzahl der Freunde, Follower oder Nachrichten sein. Somit werden unter dieser Subkategorie Teilnehmerdaten aus Data-Mining Verfahren abgedeckt, wie den user-based features von Castillo et al. oder einigen Attributen von Stringhini et al. Die Authentizität der aggregierten Informationen für einen Teilnehmer ist abhängig davon, ob die Aktions- und Accountdaten authentisch vorliegen. Des Weiteren müssen die Aktionsdaten eines Teilnehmers über einen zeitlichen Verlauf vorliegen. Wie umfangreich die Aktionsdaten aus der Vergangenheit sein müssen, ist dabei von dem jeweiligen Anwendungsfall abhängig. Dabei ist zu beachten, dass je nach Größe der zu verarbeitenden Datenmenge, mehr oder weniger Rechen- und Speicherkapazität der beteiligten Komponenten in Anspruch genommen wird.

In der zweiten Subkategorie werden die Informationen aus den Daten von mehreren Teilnehmern zusammengesetzt, wie beispielsweise die Häufigkeit der Erwähnung eines Teilnehmers aus der Arbeit von Benevenuto et al. oder auch der Teilnehmer, der die meisten Tweets zu einem Thema beziehungsweise mit einer bestimmten Menge an Worten verfasst hat, da hierfür auch die Tweets anderer Teilnehmer berücksichtig werden müssen. Um diese Subkategorie von Informationen authentisch zusammenzuführen, ist das Sammeln der Aktions- und beziehungsweise oder Accountdaten von allen betroffenen Teilnehmern erforderlich. Dies kann eine kleine abgegrenzte Menge von Teilnehmern bedeuten, wenn beispielsweise nur der Freundeskreis eines Teilnehmers oder eine kleine Gruppe von Teilnehmern betrachtet wird, allerdings auch das komplette soziale Netzwerk betreffen. Insbesondere in sozialen Netzwerken, die keine zentrale Organisationseinheit besitzen, ist dies erschwert. Einen tieferen Einblick auf die Auswirkungen durch die Dezentralisierung auf diese Kategorie wird in Abschnitt 6.3 gegeben.

4.3.4 Abgeleitete Daten

Abgeleitete Informationen beinhalten alle Teilnehmerdaten, die sich aus den vorherigen Kategorien kalkulieren oder ermitteln lassen. Dies können beispielsweise Informationen sein, die wie in den oben beschriebenen Verfahren, die Glaubwürdigkeit

eines Teilnehmers, Themas oder eines Beitrages angeben (siehe auch Tabelle 4). Um dies zu berechnen können wiederrum die Informationen vieler Teilnehmer aus dem sozialen Netzwerk erforderlich sein, weshalb hier die Kategorie mehrere Teilnehmer eingeführt wurde. Ebenso kann es sich hierbei aber auch um das Ableiten neuer Informationen aus den Daten eines Teilnehmers, wie der Grad der Übereinstimmung der Nachrichten eines Teilnehmers, wie bei Stringhini et al. handeln. Damit diese Informationen entsprechend abgleitet werden können, sind je nach Bedarf die authentischen Account- und Aktionsdaten sowie die daraus aggregierten Informationen notwendig. Des Weiteren ist das Verfahren zur Kalkulation der abgeleiteten Informationen an sich maßgebend für die Qualität der abgeleiteten Informationen.

4.3.5 Anderweitige Informationen

Zu den Informationen, die innerhalb des sozialen Netzwerkes benötigt werden, kommen noch eine Reihe von Informationen, die mit dem sozialen Netzwerk zusammenhängen, aber nicht direkt innerhalb des sozialen Netzwerkes gebraucht werden. Im Bezug auf ein Peer-to-Peer-Netzwerk (siehe hierzu Abschnitt 5.5), kann dies beispielsweise der Vertrauenswert für einen Peer in einem Netzwerk sein, der aussagt, ob sich der Peer altruistisch oder egoistisch verhält. Ebenso können dies Informationen sein, die Aufschluss über die Speicherkapazität eines Peers geben oder ob ein Peer eine hohe Verfügbarkeit und Performanz aufweist, um diesen für das Routen von Paketen zu bevorzugen. Diese Art von Informationen können je nach Infrastruktur und verwendeten Verfahren variieren.

4.4 Diskussion zur Authentizität von Teilnehmerdaten

Durch die vorhergehende Analyse können nun charakteristische Eigenschaften zur Sicherstellung der Authentizität genannt werden. Wie bereits in Abschnitt 2.4 aufgeführt, ist die Urheberschaft der Daten zu klären, was für alle Kategorien der hier entwickelten Klassifizierung zutrifft. In diesem Zusammenhang muss auch die Datenintegrität berücksichtig werden, da nur berechtigte Änderungen auch weiterhin authentische Daten ermöglichen. Dies wird unter anderem bei der Betrachtung von verdeckten Aktionen ersichtlich, die keine Indizien zur ihrer Durchführung bieten, da dies gegen das Kriterium der unbemerkten Veränderung spricht. Eine Aktion, wie der Aufruf eines Profils, ist zwar ein lesender Zugriff, kann aber zur Veränderung der Daten eines Teilnehmers führen, wenn es eine Funktion des sozialen Netzwerkes ist, die Anzahl der Profilaufrufe zu erfassen. Ein weiterer Aspekt wird durch die Betrach-

tung der Aktionsdaten (im speziellen die Fremdaktionen) ersichtlich, nämlich die Verbindlichkeit von Aktionen. Ohne Erfüllung der Anforderung des Schutzziels der Verbindlichkeit, kann ein Angreifer in der Lage sein Teilnehmerdaten unberechtigt zu erstellen, zu verstecken oder zu erfinden. Ein Beispiel für diesen Aspekt kann ein Teilnehmer sein, der eine Empfehlung eines Beitrages zurück nehmen möchte, welche er abgegeben hat. Der Teilnehmer, der empfohlen wurde, behält die Information über die Empfehlung allerdings weiterhin als Reputation in seinem Profil. Es muss also sichergestellt sein, dass Informationen auch weiterhin gültig sind. Ebenso kann ein Teilnehmer einen negativen Kommentar ignorieren und diesen auf seiner Pinnwand nicht darstellen. Daraus ergibt sich, dass die Verbindlichkeit für Teilnehmerdaten, einen wichtigen Beitrag zur Echtheit der Daten und somit zur Authentizität leistet.

Die bis hierhin genannten Punkte stellen sicher, dass Daten authentisch vorliegen. Allerdings können die repräsentierten Informationen von der Realität abweichen. Dies kann durch einfache Falscheingaben, wie beispielsweise bei einer Alters- und Namensangabe oder einer E-Mailadresse innerhalb der Profildaten getätigt werden, was sich entsprechend überprüfen lässt oder durch die Teilnehmer des sozialen Netzwerkes entdeckt werden kann. Um allerdings aggregierte oder abgeleitete Informationen, wie beispielsweise eine hohe Reputation durch viele *gefällt mir*-Angaben bei Facebook zu erreichen, muss ein Angreifer authentische Aktionsdaten erzeugen. Dies kann über einen Sybil-Angriff oder mittels konspirativ agierende Gruppen erreicht werden. Im Falle von offensichtlichen Fälschungen der Angaben, wie beispielsweise eine Altersangabe, die einen sehr hohen oder negativen Wert annimmt oder einer sehr hohen Anzahl von *gefällt mir*-Angaben, obwohl der Teilnehmer nur über einige wenige soziale Kontakte in dem Netzwerk verfügt, kann dies durch die Teilnehmer erkannt werden. Bleiben die Fälschungen allerdings in einem normalen Rahmen, kann die Erkennung möglicherweise gar nicht oder nur durch eine genaue Überprüfung der Angaben möglich sein. Hierfür ist zum einen Transparenz erforderlich, so dass die Teilnehmer ermitteln können, wer für eine Aktion verantwortlich ist. Kommen die Teilnehmer zu dem Entschluss, dass die Aktion von einem Teilnehmer durchgeführt wurde, hinter dem sich keine eigenständige Person oder Institution verbirgt, ist die Glaubwürdigkeit der Teilnehmerdaten beeinträchtigt. Somit ist die Echtheit von Teilnehmerdaten auch durch die Authentizität einer Identität bestimmt, die die Teilnehmerdaten erzeugt. Im Vergleich dazu bieten mehrere Accounts für einen Teilnehmer auch die Möglichkeit Lebensbereiche von einander zu trennen. So kann beispielsweise ein Teilnehmer einen zweiten Account besitzen, um sein berufliches Umfeld von seinem privaten zu unterscheiden. Dies kann zwar in

sozialen Netzwerken bedingt durch die Einteilung der sozialen Kontakte in Gruppen erreicht werden, allerdings stößt dieses Konzept meist auf Grenzen, wie bei der Anzeige, welcher Nutzer online ist, oder dass jeder soziale Kontakt des Teilnehmers das gleiche Profilbild angezeigt bekommt. Somit gilt es abzuwägen, welche Relevanz die Sicherstellung die Echtheit der Daten aufweist, da dies zum einen sehr aufwendig sein kann und zum anderen zur Verletzung der Privatsphäre oder Einschränkungen der Freiräume führen kann.

Bei den abgeleiteten und aggregierten Daten sind die Ergebnisse abhängig von den Kategorien Account- und Aktionsdaten. Da diese aus den Daten der beiden vorher genannten Kategorien gebildet werden, können sie als authentisch angesehen werden, insofern dies für die vorliegenden Account- und Aktionsdaten angenommen werden kann.

Beim Aufstellen der Kategorien bestand die Möglichkeit Account- und Aktionsdaten auch nach der Sichtbarkeit einzuordnen. Hierauf wurde weitestgehend verzichtet, da sich die Sichtbarkeit der Daten für die Teilnehmer zum einen von der Plattform und zum anderen von der Benutzerschnittstelle abhängig sind. Es ist auch durchaus möglich, dass mehr Daten bei einem Teilnehmer liegen, als ihm von der visuellen Schnittstelle angezeigt wird. Somit erlaubt die Verwendung der Sichtbarkeit als Kriterium nur eine geringe Trennschärfe für die Einteilung der Ausprägungen von Teilnehmerdaten. Allerdings können bei sichtbaren Merkmalen die Daten von anderen Teilnehmern eingesehen werden und unterstehen somit einer Kontrolle des sozialen Netzwerkes. Dies kann dazu führen, dass Teilnehmer deren Daten nicht plausibel erscheinen, von aufrichtigen Teilnehmern gemieden werden.

4.5 Zusammenfassung

Innerhalb dieses Kapitels wurde eine Einführung in den Data Mining-Prozess geben und aktuelle wissenschaftliche Publikationen und Verfahren vorgestellt, welche Teilnehmerdaten in sozialen Netzwerken verwenden. Mittels der gewonnen Erkenntnisse wurde eine eigene Klassifikation zu Teilnehmerdaten entworfen, welche den Fokus auf die Unterscheidbarkeit der Daten nach den Merkmalen zur Authentizitätsprüfung legt. Dabei konnte festgestellt werden, dass die Authentizität der Teilnehmerdaten unter anderem durch den Urhebernachweis, Sicherstellung der Integrität und der Echtheit der Informationen über die Verbindlichkeit von Aktionen bestimmt ist. Des Weiteren kann die Identität eines Teilnehmers Einfluss auf die Glaubwürdigkeit von Teilnehmerdaten haben. Für die Sicherstellung der Echtheit von Informationen,

wurden schon erste Verfahren für die Kategorien Account- und Aktionsdaten genannt. Um die Zielstellung dieser Arbeit weiter zu bearbeiten, ist es erforderlich, die hier gewonnen Erkenntnisse im Zusammenhang mit sozialen Netzwerken ohne eine zentrale Organisationseinheit im nächsten Kapitel zu betrachten.

5 Auswirkung der Dezentralisierung auf die Teilnehmerdaten

Dieses Kapitel geht auf die verschiedenen Formen der Dezentralisierung von sozialen Netzwerken ein und zeigt, inwieweit die Anforderungen aus den vorherigen Kapiteln umgesetzt werden. Um die Auswirkung der Dezentralisierung auf die Teilnehmerdaten zu analysieren, erfolgt eine Betrachtung darüber, wie die Teilnehmerdaten der jeweiligen Kategorien aus Kapitel 4 in den einzelnen Formen der Dezentralisierungen gesichert werden. Aus dieser Analyse heraus werden Bereiche identifiziert, in denen Maßnahmen zur Erfüllung der relevanten Schutzziele eingesetzt werden können.

5.1 Dimensionen der Dezentralisierung

Um die Auswirkungen der Dezentralisierung von sozialen Netzwerken auf die Teilnehmerdaten zu erheben, werden in diesem Abschnitt die unterschiedlichen Formen der Dezentralisierung vorgestellt. Nach Paul et al. [51] lassen sich drei architekturelle Eigenschaften nennen, durch welche sich die verschiedenen Formen einordnen lassen. Die erste Eigenschaft bezieht sich auf die Art der Infrastruktur des sozialen Netzwerkes. Eine Plattform kann über die Server einer zentralen Organisationseinheit mittels dezentraler Server oder auf Basis eines P2P-Netzwerkes betrieben werden. Die zweite Eigenschaft bezieht sich auf die Datenhaltung, wobei entweder ein Teil der Daten lokal bei den einzelnen Clients oder alle Daten fernverwaltet auf den Servern liegen. Die letzte Eigenschaft umfasst die Kommunikation zwischen den Teilnehmern. Dabei ist zu unterscheiden, ob die Kommunikation direkt zwischen den Teilnehmern oder über Zwischenstation, wie Servern oder Overlays, stattfindet. Durch die Kombination dieser Eigenschaften lassen sich acht Kategorien aufstellen, welche in Tabelle 1 dargestellt sind. Von diesen acht Kategorien wird die Kategorie soziale Netzwerke mit einer zentralen Organisationseinheit vorgestellt, da diese Form beim Verständnis und für den direkten Vergleich weiterhiflt. Des Weiteren werden die Ansätze von dezentralen Servern (siehe c in Tabelle 1), P2P-Netzwerken (g und h) und zentrale Systeme mit P2P-Unterstützung (b) vorgestellt. Nicht tiefergehend behandelt werden in diesem Kapitel Schnittstellendienste (e), da diese es den Teilnehmern ermöglichen, Accounts aus verschiedenen sozialen Online-Netzwerken mittels einer Plattform übergreifend zu nutzen, allerdings kein eigenes soziales Netzwerk darstellen sowie alle restlichen noch nicht genannten Kategorien (siehe Zeile d und f), da zu diesen Kategorien bis zu diesem Zeitpunkt noch keine relevante

Umsetzung gefunden werden konnten.

Dezentral.	**Datenhaltung**	**Komm.**	**Ausprägung**
Zentral	Fernverwaltet	Indirekt	a) Soziale Netzwerke mit einer zentralen Organisationseinheit
		Direkt	b) Soziales Netzwerk mit einer zentralen Organisationseinheit unterstützt von einem P2P-Netzwerk
Dezentrale Server	Fernverwaltet	Indirekt	c) Dezentrale Server
		Direkt	d) wie c) mit Unterstützung von P2P-Systemen
	Lokal	Indirekt	e) Schnittstellendienste für soziale Netzwerke
		Direkt	f) wie e) mit Unterstützung von P2P-Systeme
Peer-to-Peer	Lokal	Indirekt	g) P2P-Systeme mit indirekter Kommunikation
		Direkt	h) P2P-Systeme mit direkter Kommunikation

Tabelle 1: Klassifikation sozialer Netzwerke modifiziert aus [51]

5.2 Zentrale Organisationseinheit

Bei einem sozialen Netzwerk mit einer zentralen Organisationseinheit findet die gesamte Kommunikation über Zwischenstationen statt. Bei den Zwischenstationen handelt es sich um Server des Anbieters, die die dabei entstehenden Daten für einen Dienstanbieter sammeln, auch wenn die Kommunikation über verschiedene Server abgewickelt wird (siehe Abbildung 6). Die Verwendung von Zwischenstationen hat den Vorteil, dass alle Aktionen über eine dritte Instanz gehen, welche die Durchführung einer Aktion bezeugen kann. Somit können die Teilnehmer davon ausgehen, dass die Aktionsdaten, die beispielsweise auf der Profilseite eines Teilnehmers angezeigt werden, korrekt sind, solange die Teilnehmer dem Anbieter des sozialen Netzwerkes vertrauen, dass dieser sie nicht verändert hat. Änderungen, die der Dienstanbieter an den Teilnehmerdaten durchführt, müssen angemessen sein, da sonst die Gefahr eines Vertrauensverlustes der Teilnehmer in den Anbieter besteht. Eine angemessene Veränderung kann unter anderem vorkommen, wenn der Teilnehmer gegen die Vereinbarungen verstößt, denen der Teilnehmer für die Nutzung des sozialen Netzwerkes zugestimmt hat, wie beispielsweise die Verbreitung kriminel-

ler Inhalte durch den Teilnehmer innerhalb der Plattform. Ist die Veränderung der Teilnehmerdaten in dem Bewusstsein der Teilnehmer unangemessen, kann dies zum Vertrauensverlust führen, auch wenn die vorher durchgeführte Aktion gegen die Nutzungsbedingungen des Anbieters verstößt. Das Vertrauen in einen zentralen Anbieter ist allerdings nicht immer von Grund auf gegeben, denn der Anbieter wird möglicherweise von dem Gesetzgeber des jeweiligen Landes beeinflusst und verfolgt zudem seine eigenen Interessen, welche unter anderem finanziell begründet sind. Durch die Rechtsgrundlage und Behörden eines Staates kann Einfluss auf einen Anbieter genommen werden, um das soziale Netzwerk zur Überwachung zu nutzen. Des Weiteren kann der Anbieter die Beiträge jederzeit einsehen und gegebenenfalls zensieren. Um dem Mitlesen der Inhalte vorzubeugen, existieren Lösungsansätze, welche die Inhalte mittels kryptographischer Verfahren verschlüsseln, bevor sie an das soziale Netzwerk gesendet werden. Andere Ansätze versuchen die Zensur von Beiträgen zu erschweren, indem Beispielsweise die Zuordnung der Themen von Beiträgen vermischt wird [4]. Da dieser Ansatz auf die Verschlüsselung der Inhalte setzt, sind für den Dienstanbieter Inhalte der Eigen- und Fremdaktionen nicht mehr verfügbar sowie Informationen, die aus den Inhalten hervorgehen. Der Anbieter kann allerdings weiterhin die Semantik der Eigen- und Fremdaktionen sowie einen Teil der Metainformationen beziehen. Bei den Metainformationen können zusätzlich die Informationen über die Kommunikationsteilnehmer verloren gehen, wenn die Zugriffskontrolle für einen Beitrag nicht mehr über das soziale Netzwerk, sondern über die Verschlüsselung erfolgt. Dies kann erreicht werden, indem ein Beitrag für alle Teilnehmer freigegeben wird, aber nur eine bestimmte Teilmenge der Teilnehmer den Beitrag entschlüsseln kann. Dies hat allerdings den Nachteil, dass Teilnehmer, die keine Berechtigung haben die Nachricht zu entschlüsseln, von den nicht lesbaren Nachrichten störend beeinflusst werden oder sich ausgeschlossen fühlen können. Des Weiteren ist zu beachten, dass der Austausch von den Schlüsseln zur Ver- und Entschlüsselung über einen anderen Kanal als dem genutzten sozialen Netzwerk getätigt wird, da ansonsten Rückschlüsse auf die Teilnehmer und deren Beziehungen sowie ein Man-in-the-Middle-Angriff möglich sind. Hinsichtlich der praktischen Umsetzung ergibt sich der Nachteil, dass kryptographische Verfahren zu höheren Zugriffszeiten [5] führen können. Des Weiteren muss jeder Teilnehmer entsprechende Werkzeuge auf seinem System einrichten oder Dienste nutzen, wenn mittels verschlüsselter Nachrichten innerhalb der Plattformen kommuniziert werden soll, solange diese Maßnahmen nicht in dem sozialen Netzwerk integriert sind. Dies führt gegebenenfalls zum Ausschluss von Nutzern, die an der technischen Hürde oder aus anderen Gründen scheitern, diese Werkzeuge zu

verwenden.

Die Accountdaten sind abhängig davon, was die jeweilige Plattform für Daten bezieht und welche der Teilnehmer von sich preisgibt. Die Echtheit der statischen Daten für einen Account kann dabei durch die zentrale Organisationseinheit gewährleistet werden, solange die anderen Teilnehmer dem Anbieter vertrauen, dass diese nicht verändert wurden. Des Weiteren kann der Anbieter als Kontrollinstanz dienen und die Echtheit der Profildaten durch eine Überprüfung der Identität der Teilnehmer oder automatische Kontrollen der Verwaltungsdaten sicherstellen. Dies kann allerdings in sozialen Netzwerken, bei denen die Teilnehmer Wert auf Anonymität legen, zu Konflikten führen. Dabei ist Anonymität nicht nur gegenüber dem sozialen Netzwerk, sondern auch gegenüber dem Dienstanbieter gemeint. Dies wird insbesondere in der zweiten sozial-politischen Situation aus Abschnitt 3.1 wichtig, da die Teilnehmer hier mittels der Verwendung von Pseudonymen und Anonymisierungswerkzeuge, wie beispielsweise Tor[20], versuchen können, sich zu schützen.[21] Damit die Überprüfung durch einen Anbieter funktionieren kann, müssen die Teilnehmer wiederrum dem Anbieter vertrauen. Dies bietet aber auch den Vorteil, dass die Teilnehmer bei Problemen einen Ansprechpartner haben und eine Instanz existiert, die in der Lage ist, Accounts auszuschließen, wenn diese Identitätsdiebstahl oder Missbrauch betreiben. Aggregierte und abgeleitete Information können, insofern die Account- und Aktionsdaten vorhanden sind, aus einem einzigen Repository bezogen werden, wenn Zugriff auf dieses besteht. Dies erleichtert die Durchführung von Auswertungen und Data Mining-Verfahren im Vergleich zu den anderen Formen der Dezentralisierung. Allerdings ist die Kehrseite, dass die Teilnehmer keinen Einfluss darauf haben, mit welchem Ziel, wie häufig und von wem ihre Daten ausgewertet werden.

5.3 Zentrale Organisationseinheit mit Peer-to-Peer-Unterstützung

Ein soziales Netzwerk mit einer zentralen Organisationseinheit kann durch ein zusätzliches P2P-Netzwerk unterstützt werden. Somit ist es möglich, Daten nicht nur über die Infrastruktur der zentralen Organisationseinheit zu versenden, sondern auch einen Teil der Datenlast auf die Peers zu verteilen. Dadurch lassen sich beim Anbieter Kosten reduzieren, die sonst für weitere Server, deren Kühlung, Stromversorgung,

[20] https://www.torproject.org/, letzte Sichtung 30.11.2013

[21] Trotzdem ist es nicht ausgeschlossen, dass der Teilnehmer über andere Informationen von der Organisationseinheit identifiziert werden kann.

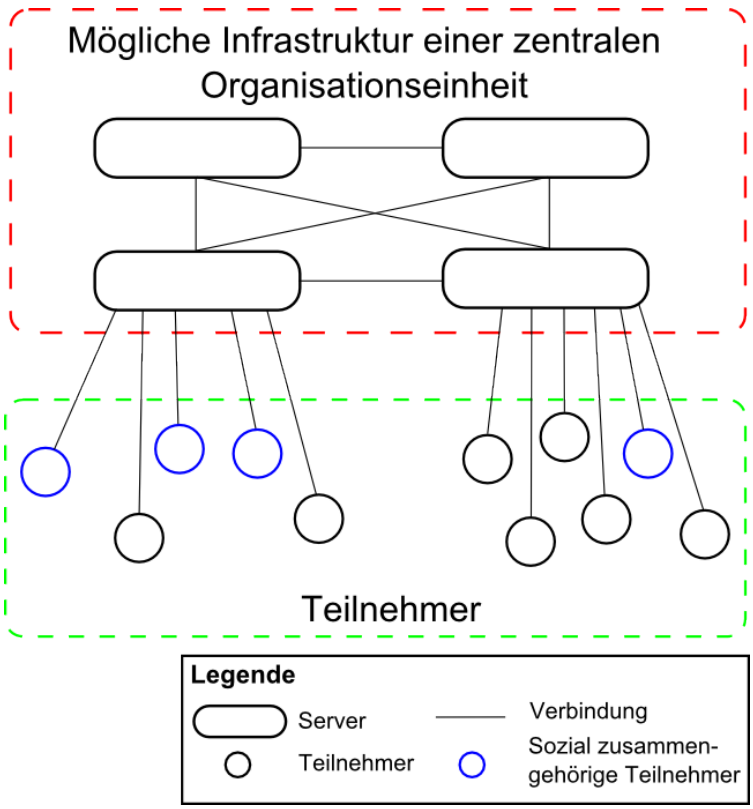

Abbildung 6: Schematischer Überblick zu einem sozialen Netzwerk mit einer zentralen Organisationseinheit

Wartung und Administration anfallen würden, um die Datenlast handzuhaben. Eine weitere Motivation kann dabei sein, das Ausfallrisiko zu verringern, da bei einem Ausfall der Server der zentralen Organisationseinheit, die Peers untereinander weiter kommunizieren können. Durch die Verwendung des P2P-Netzwerkes entsteht allerdings eine weitere Angriffsfläche für bösartige Teilnehmer und externe Angreifer. Dies führt dazu, dass das soziale Netzwerk zusätzlich gegen mögliche Angriffe auf der P2P-Ebene gesichert werden muss. Ein möglicher Angriff kann hierbei das Versenden von Nachrichten, wie etwa Spam oder Schadsoftware über das P2P-Netzwerk, sein. Dabei ist es möglich, dass die zentrale Organisationseinheit dies nicht mitbekommt, wenn Teilnehmer Nachrichten erstellen und abrufen können, da die Kontrolle der zentralen Organisationseinheit entfällt. Eine weitere Hürde kann entstehen, wenn die Teilnehmer eine Anwendung runterladen müssen, obwohl die Plattform auch über den Browser nutzbar ist. Somit müssen gegebenenfalls erst Anreize geschaffen werden, die die Teilnehmern zur Nutzung der Applikation motivieren.

Zwei Arbeiten, die innerhalb dieser Kategorie von sozialen Netzwerken existieren, sind user-assisted OSN (uaOSN) [44] und Cuckoo [67] (siehe Abbildung 7). Bei beiden Ansätzen wird das Ziel verfolgt, die Infrastruktur eines Anbieters zu entlasten. uaOSN lagert hierfür Inhalte wie Nachrichten, Videos, und Bilder auf die Geräte (Router oder Endgeräte) der Teilnehmer aus. Da das Geschäftsmodell des Anbieters allerdings darin liegt, Informationen über die Teilnehmer zu beziehen, um diese für Marketing- oder ander Zwecke zu verwenden, soll weiterhin der Anbieter über jede Aktion informiert werden. Aus diesem Grund wird der Anbieter als Verzeichnisdienst verwendet, da er zum einen die Information darüber besitzt, wo die Daten gespeichert sind, die ein Teilnehmer anfragt und zum anderen weiterhin alle nötigen Informationen speichert, die zur Darstellung von Profilen notwendig sind. Hierzu gehören unter anderem die Accountdaten, soziale Kontakte und Aktionsdaten. Durch diese Designentscheidung ist es für das P2P-Netzwerk nicht möglich eigenständig zu agieren, außer für die Daten, die die Teilnehmer auf den eigenen Geräten haben oder deren Adresse sie kennen. Bei einem Ausfall der zentralen Organisationseinheit fällt auch das restliche soziale Netzwerk aus. Die Infrastruktur von Cuckoo dagegen, kann die Funktionalität des sozialen Netzwerkes auch bei einem Ausfall der zentralen Organisationseinheit ermöglichen. Hierbei wird gezielt die Plattform Twitter adressiert, indem die Verbreitung von Profilen und Tweets über das P2P-Netzwerk getätigt wird. Die Peers organisieren sich hierfür über eine verteilte Hashtabelle (zu engl. Distributed Hash Table, kurz DHT). Eine DHT ermöglicht das Ablegen von Objekten über mehrere Peers, wobei jeder Peer und jedes Objekt eine eindeutige ID bekommt. Ein Peer ist für einen bestimmten Anteil von Objekten zuständig, die zu einem ID-Bereich gehören [14, S. 168]. Damit die Suche der Objekte in dem DHT eine bestimmte Laufzeit erreicht, werden die Peers in Gruppen oder geometrische Objekte angeordnet. Eine detailliertere Beschreibung zu DHTs wird in Abschnitt 5.5 vorgenommen. Meldet sich ein Teilnehmer in Cuckoo bei dem sozialen Netzwerk an, so bezieht dieser von den anderen Teilnehmern in dem DHT die neuen Beiträge der Teilnehmer, denen er folgt. Kann der Teilnehmer Beiträge nicht finden, agieren die Twitterserver als Datensicherung und beantworten Anfragen aus dem P2P-Netzwerk. Damit dieser Schritt möglich ist, muss jeder neue Beitrag eines Teilnehmers an die Twitterserver übertragen werden. Dies ist auch notwendig, damit andere Teilnehmer, die über die Twitter-Website oder Twitter-Applikationen den Dienst verwenden, über die Änderungen informiert werden können. Neue Beiträge sendet der Teilnehmer mittels direkter Verbindungen an seine Follower oder lässt diese mittels Gossip-Verfahren zwischen den Nachbarn verbreiten, wenn der

Teilnehmer über eine sehr große Anzahl an Follower verfügt.

Da beide Verfahren mit bereits bestehenden sozialen Netzwerken mit zentralen Organisationseinheiten zusammenarbeiten bzw. diese erweitern, unterstehen sie der Vorgabe, die Geschäftsmodelle der Anbieter der sozialen Netzwerke zu wahren. Dies führt dazu, dass Daten der Teilnehmer an die Anbieter übertragen werden, womit in dieser Form der Dezentralisierung, ein Modell in dem die Privatsphäre der Nutzer gewahrt wird, schwer vorstellbar ist. Eine zentralen Organisationseinheit kann dafür als Backup oder vertrauenswürdige Instanz agieren, welche die Vorteile zentraler Organisationseinheiten mit sich bringt, wenn es unter anderen um die Sicherheit in dem P2P-Netzwerk geht, wie beispielsweise eine Public-Key-Infrastruktur (PKI) zu integrieren. Da die Teilnehmer sich immer noch über die zentrale Organisationseinheit registrieren, können auch weiterhin die Verfahren zur Sicherung der Accountdaten angewendet werden. Die statischen Daten können ebenso weiterhin über die zentrale Organisationseinheit gewährleistet werden. Bei den Aktionsdaten sind die Inhalte im Fall von uaOSN nicht mehr bei der zentralen Organisationseinheit gespeichert. Somit ist es möglich, dass Teilnehmer diese modifizieren oder austauschen, ohne die zentrale Organisationseinheit zu benachrichtigen. Des Weiteren gehen für die zentrale Organisationseinheit die Metadaten verloren, die sich aus den Inhalten der Aktionsdaten beziehen lassen, vorausgesetzt die zentrale Organisationseinheit lädt die Inhalte für jede Datei nicht noch einmal zusätzlich herunter. Hinsichtlich der Aktionsdaten ist es möglich, dass ein Teilnehmer eine Datei mehrfach aufruft, sobald der Teilnehmer den Speicherort der Datei bezogen hat, so dass die zentrale Organisationseinheit keinen Überblick mehr über die Häufigkeit der Zugriffe auf eine Datei hat. Bei Cuckoo werden die Änderungen ebenfalls über das P2P-Netzwerk übertragen und an das soziale Netzwerk gesendet. Somit kann die zentrale Organisationseinheit zwar alle Änderungen beobachten, hat aber keine gesammelten Informationen mehr darüber, wer auf welche Daten zugreift, weshalb die Autoren vorschlagen, Statistiken über das Nutzungsverhalten von den Peers an den Anbieter weiterzuleiten. Da beide Verfahren die Teilnehmerdaten über eine zentrale Instanz speichern, bietet es sich an, hier auch aggregierte und abgeleitete Informationen über die zentrale Organisationseinheit zu beziehen.

5.3.1 Diskussion der Sicherheitsmaßnahmen

Die Betrachtung der beiden Verfahren ergibt, dass bei dieser Form der Dezentralisierung, jeweils für die Kategorien von Daten, die über das P2P-Netzwerk übertragen

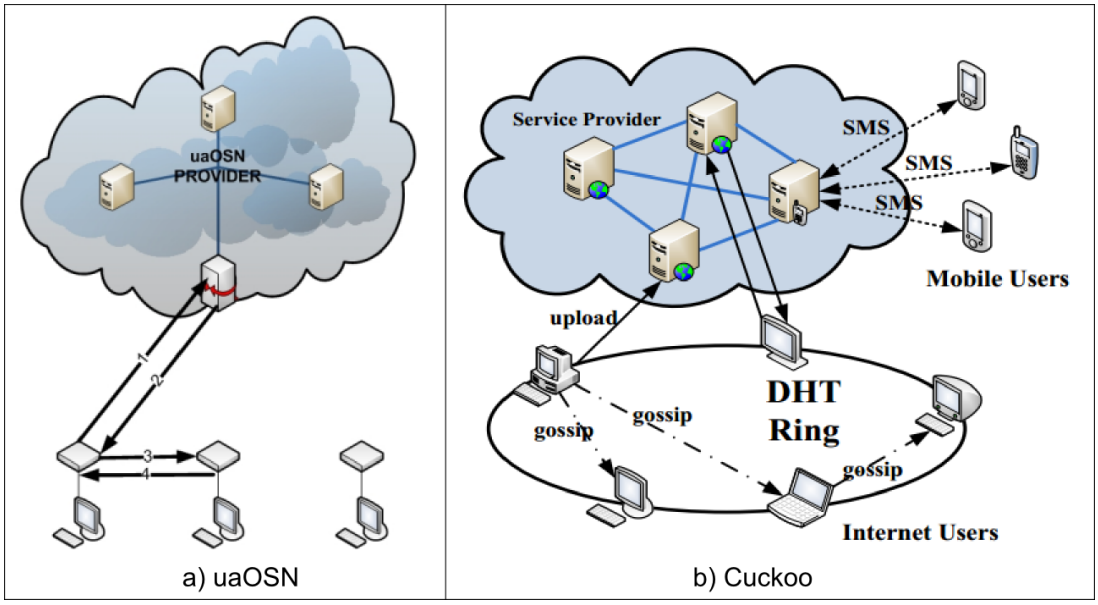

Abbildung 7: Systemarchitektur von Cuckoo und uaOSN aus [44, 67]

werden, Maßnahmen eingeleitet werden müssen, wenn die Sicherstellung der Authentizität und Integrität der Daten eine Rolle spielt. Bei uaOSN werden nur die Inhalte bei den Teilnehmern ausgelagert, weshalb die Inhalte auf Authentizität und Integrität zu prüfen sind. Eine Möglichkeit hierfür könnte die Erstellung eines Hashwertes durch die zentrale Organisationseinheit mittels einer Hash-Funktion sein. Dafür müssen die Dateien einmal an die zentrale Organisationseinheit übertragen oder der Speicherort angegeben werden, damit diese einen Hash-Wert erstellen und signieren kann. Der signierte Hash-Wert kann dann zu der Datei abgelegt werden oder ohne Signatur zu dem Eintrag über den Speicherort der Datei auf der zentralen Organisationseinheit ablegt werden. Andere Teilnehme können dann anhand der Datei, des angegebenen Hash-Wertes und einer eigenen Berechnung des Hash-Wertes der Datei überprüfen, ob die Datei verändert wurde. In dem Prozess zur Berechnung des Hash-Wertes kann der Anbieter auch wieder Informationen über die Inhalte erfassen und gleichzeitig die Daten auf Schadsoftware oder Spam untersuchen. Nichtsdestotrotz geht dabei ein Teil der gewonnenen Performanz wieder verloren. Des Weiteren muss bei der Übertragung zwischen dem Teilnehmer und der zentralen Organisationseinheit sichergestellt werden, dass die Kommunikationspartner authentisch sind und die der Inhalt auf dem Übertragungsweg nicht verändert wurden. Hierfür bieten sich die Authentifizierung beispielsweise mittels Benutzername und Passwort

sowie die Verwendung des TLS bzw. dem Vorläufer des SSL-Protokolls an, wie es auch bei sozialen Netzwerken mit einer zentralen Organisationseinheit ohne P2P-Unterstützung teilweise gemacht wird.[22] Bei Cuckoo können Daten direkt von einem Peer aus dem DHT bezogen werden, was dazu führt, dass der Peer die Einträge, die er speichert, verändern kann. Die Autoren schlagen hierfür vor, Beiträge mit einer digitalen Signatur zu versehen. Des Weiteren können Beiträge eines Blogs von einem Peer verheimlicht bzw. geblockt werden, wofür sich Hash-Ketten aus [54] verwenden lassen (siehe Abschnitt 6.1.3). Eine andere Möglichkeit ist, dass ein Nutzer falsche Angaben zu seinem Profil macht, wie zu der Anzahl seiner Follower. Hierfür ist es möglich die zentrale Organisationseinheit mit einzubeziehen, indem die Daten in einer Anfrage überprüft werden. Ein weiterer Angriff ist möglich, wenn ein Teilnehmer Änderungen in dem P2P-Netzwerk vornimmt, diese aber nicht an die zentrale Organisationseinheit übermittelt. Somit entstehen Inkonsistenz bei den Daten. Als letztes lassen sich noch die Aktionsdaten nennen, die für den Anbieter durch die Interaktion der Teilnehmer in dem P2P-Netzwerk nicht ersichtlich sind. Die Statistiken über das Nutzungsverhalten können von den Peers gefälscht werden. Eine Überprüfung über die Echtheit dieser Informationen ist möglich, wenn jeder Teilnehmer Aussagen über sich selbst und über das Verhalten der anderen Teilnehmer tätigt. Wird bei diesem Prozess Inkonsistenz entdeckt, kann der Anbieter sich die Aktionen[23] der jeweiligen Peers zukommen lassen, um zu überprüfen, welche von diesen Aktionen stattgefunden haben. Hierfür sind allerdings kryptographische Verfahren erforderlich, damit die Authentizität, Integrität und Verbindlichkeit sichergestellt werden. Dies führt zu einem höheren Aufwand und somit zu einer stärkeren Beanspruchung der zentralen Organisationseinheit sowie mehr Speicherplatzbedarf auf den Peers oder den Servern der zentralen Organisationseinheit, um die Aktionen nachweisen zu können. Zwischen der zentralen Organisationseinheit und den Teilnehmern können ebenfalls wieder Verschlüsselungstechniken wie TLS bzw. SSL eingesetzt werden.

5.4 Dezentrale Server

Bei dieser Dezentralisierungsform besitzt ein soziales Netzwerk mehr als eine Organisationseinheit, welche das Netzwerk betreibt. Die Server der Organisationseinheiten ermöglichen das Speichern und Verwalten der Accounts der Teilnehmer, wobei ein Server mehrere Teilnehmer aufnehmen kann oder ein Teilnehmer einen eigenen Server besitzt. Die Clients kommunizieren über die Server und nicht direkt miteinander.

[22] Bei einem Zugriff über den Browser wird TLS/SSL mittels HTTPS verwendet
[23] Ein Peer zeigt, welche Nachrichten er in dem Netzwerk verschickt hat.

Um dies umzusetzen, müssen die Server eine Möglichkeit haben, Teilnehmer des gleichen sozialen Netzwerkes auf anderen Servern zu kontaktieren. Hierfür können die Server in Strukturen geordnet oder Adressierungen verwendet werden. Ein Adressierung der Server kann beispielsweise durch DNS umgesetzt werden, wie es bei XMPP [53, S. 14-15] der Fall ist. Die Teilnehmer haben hierfür eine eindeutige Adresse, mit der sie identifiziert werden können und der Name des Servers erkennbar ist.[24] Somit ist es möglich, dass der Server des Absenders einer Nachricht eine direkte Verbindung zu dem Server des Empfängers der Nachricht aufbaut (siehe Abbildung 8). Alternativ kann allerdings auch eine Nachricht über mehrere Zwischenstationen zu einem Ziel geleitet werden. Das Weiterleiten über mehrere Maschinen führt dazu, dass jede Station, die die Nachricht durchläuft, entsprechende Angriffe durchführen kann, wie das Einsehen des Inhaltes, Blocken oder Verändern der Nachricht (siehe Abbildung 9). Dies kann auch bei der direkten Kommunikation zwischen den Servern passieren, vorausgesetzt die beiden Teilnehmer verwenden nicht den gleichen Server. Allerdings sind bei dieser Variante die Zwischenstationen auf zwei Server begrenzt. Verfahren wie TLS bzw. SSL, welche sich in sozialen Netzwerken mit einer zentralen Organisationseinheit anbieten, sind für die sichere Übertragung weniger geeignet, da sie keine Ende-zu-Ende-Verschlüsselung der Daten anbieten, sondern nur zwischen den beiden Kommunikationsteilnehmern, die gerade die Daten austauschen. Somit sind die Daten nur zwischen dem Server und dem Teilnehmer oder zwischen den beiden Servern verschlüsselt und liegen danach dem jeweiligen Server ungeschützt vor, bis sie für die nächste Übertragung oder zum Speichern wieder verschlüsselt werden. Die Teilnehmer müssen also nicht nur dem Server vertrauen, der für das Speichern und Verwalten des eigenen Accounts zuständig ist, sondern auch allen weiteren Zwischenstationen, bis hin zum Empfänger. Um das Risiko von Missbrauch zu verringern, bleibt die Möglichkeit kryptographische Verfahren zu verwenden. Dabei muss unterschieden werden, ob die kryptographischen Verfahren zur Sicherung der Integrität, Authentizität und Verbindlichkeit schon beim Teilnehmer oder erst bei dem Server ansetzen. Hat der Server vollen Zugriff auf die Daten sowie die Möglichkeit, selbst im Namen des Teilnehmers zu verschlüsseln, kann dieser auch entsprechende Angriffe durchführen. Darüber hinaus ist es möglich, dass ein Server sich für längere Zeit aufrichtig verhält und später sein Verhalten negativ verändert. Dieser Aspekt fällt allerdings nach Paul et al. nicht so stark ins Gewicht, da das Vertrauen weniger von dem Verhalten, sondern von der Reputation der Organi-

[24] Als Beispiel kann hier das Adressierungsschema von Diaspora angeführt werden, wobei eine Teilnehmeradresse nach dem Schema 'Nutzername'@'Serveradresse' aufgebaut ist [25].

sationseinheit abhängt. Trotzdem sollte nicht nur ein Server verwendet werden, da ansonsten alle Daten der Teilnehmer betroffen sind, wenn dieser doch sein Verhalten ändert und die Daten löscht.

Ein Ziel dieser Dezentralisierungsform ist es zu verhindern, dass eine Organisationseinheit Zugriff auf die Daten aller Teilnehmer hat. Somit haben die Server nur Zugriff auf die Daten der Teilnehmer, deren Account bei der jeweiligen Organisationseinheit angesiedelt ist. Jeder Server hat dabei für seine Teilnehmer den gleichen Zugriff, wie eine Organisationseinheit in einem zentral gehaltenen sozialen Netzwerk. Wird allerdings eine Ende-zu-Ende-Verschlüsslung vom Client aus verwendet, können je nach dem Anteil der verschlüsselten Daten, die Inhalte der Aktionsdaten bis hin zu allen Daten, außer den Metadaten der Aktion, für den Server verborgen bleiben. Sobald alle Daten verschlüsselt werden, auch um welche Art von Aktion es sich handelt, dient der Server nur noch als Speicher und Übertragungsmedium. Dabei kann der Server protokollieren, wer welche Daten, zu welchem Zeitpunkt abruft oder speichert und wie groß die Daten sind. Dadurch wird allerdings auch der Aufgabenbereich des Servers eingeschränkt, da dem Server beispielsweise keine Informationen mehr über das soziale Netzwerk eines Teilnehmers vorliegen und somit andere Teilnehmer nicht mehr aktiv benachrichtigen kann, über neue Nachrichten oder wenn ein Teilnehmer verfügbar ist. Des Weiteren muss der Server in der Lage sein, zu unterscheiden, bei welchen der Schreibzugriffen es sich um eine berechtigte Anfrage handelt, um Daten zu verändern, hinzuzufügen oder zu löschen. Ebenso gehen serverseitige Kontrollmöglichkeiten verloren, da der Server die Aktionen nicht mehr eindeutig einordnen kann. Je nach Reichhaltigkeit der Account- und Aktionsdaten variieren auch wieder abgeleitete und aggregierte Informationen. Allerdings ist es in dieser Dezentralisierungsform, auch ohne Ende-zu-Ende-Verschlüsselung erschwert aggregierte Informationen zu beziehen, wenn die Daten mehrere Teilnehmer umfassen, insbesondere wenn diese zu einer anderen Organisationseinheit gehören. Die Daten von Teilnehmern einer anderen Organisationseinheit, werden dabei nur bezogen, wenn eine Interaktion zwischen einem eigenen Teilnehmer und einem Teilnehmer der anderen Organisationseinheit kommt. Somit fällt ein weiterer Teil der abgeleiteten Informationen bzw. die Kombination aus beiden Kategorien weg. Bei einem System, wie Vis-à-Vis [57] wird dieser Umstand weiter verstärkt, da hier jeder Teilenehmer genau einen *Virtual Individual Server* (VIS) besitzt. Ein VIS wird dabei auf einem Cloud-Dienst[25] oder selbst verwalteten Server betrieben, welcher allerdings mit Kosten für jeden Teilnehmer verbunden ist. Die Autoren gehen davon

[25] wie Amazon EC2 https://aws.amazon.com/de/ec2/, letzte Sichtung 30.11.2013

aus, dass keine Verletzungen der Privatsphäre durch die Anbieter der Cloud-Dienste begangen werden, da die Teilnehmer für die Dienste zahlen und das Geschäftsmodell der Cloud-Dienste nicht aus der Vermarktung der Daten der Teilnehmer besteht. Die Verlagerung der Teilnehmer auf jeweils einen Server führt dazu, dass sich der Überblick über das soziale Netzwerk nur noch auf die eigenen Daten und die Daten, die andere Teilnehmer freigeben möchten beschränkt. Dies erschwert das Beziehen von aggregierten Daten, die sich auf mehrere Teilnehmer beziehen.

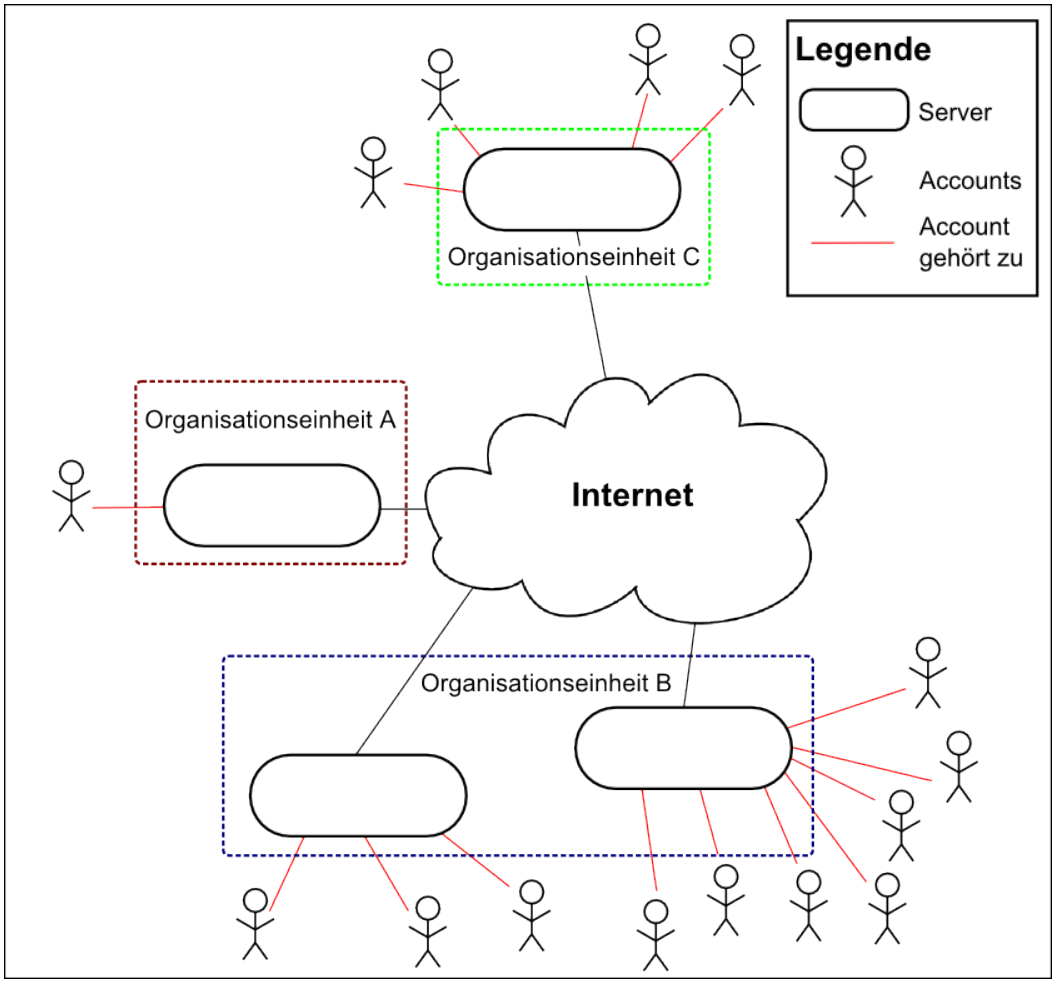

Abbildung 8: Schematischer Überblick eines sozialen Netzwerkes mit dezentralen Servern ohne eine feste Hierarchie modifiziert aus [26]

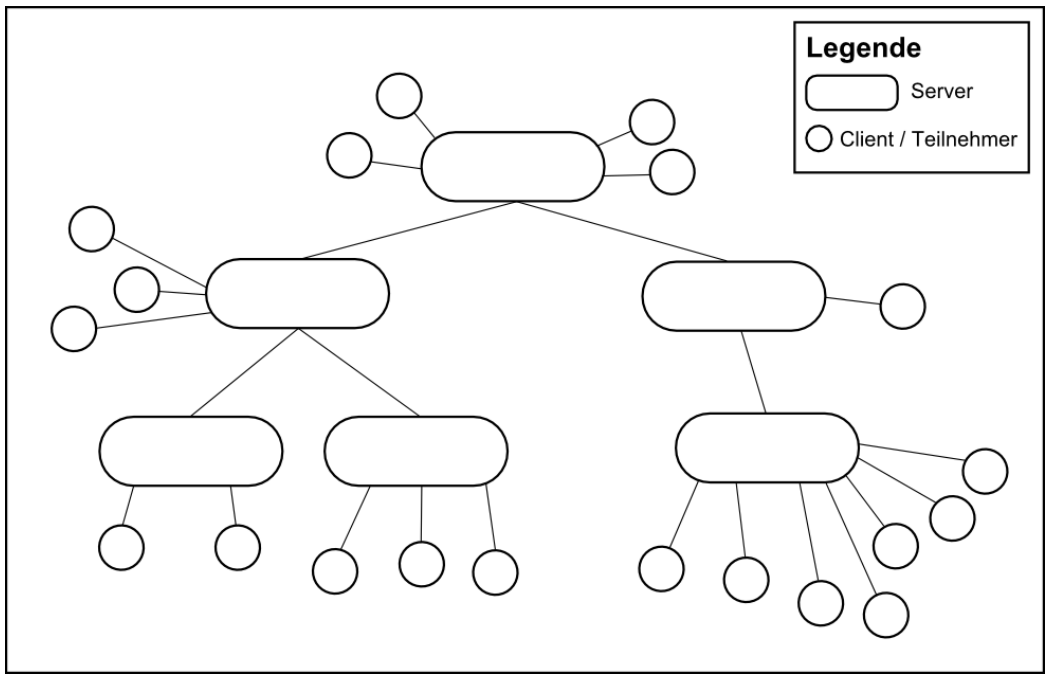

Abbildung 9: Schematischer Überblick eines sozialen Netzwerkes mit dezentralen Servern mit einer festen Hierarchie ohne Kennzeichnung von Organisationseinheiten

5.4.1 Diskussion der Sicherheitsmaßnahmen für soziale Netzwerke mit dezentralen Servern

Innerhalb dieser Dezentralisierungsformen gibt es mehrere Varianten, die jeweils verschiedene Maßnahmen benötigen. Bei dem Verzicht auf kryptographische Maßnahmen, außer für den Übertragungsweg zwischen zwei Stationen[26], beruht die Korrektheit der Daten auf Vertrauen gegenüber der jeweiligen Organisationseinheiten. Ein sich bösartig verhaltender Server ist dabei in der Lage, die Daten nach Belieben zu ändern, was danach nur durch Überprüfungen, beispielsweise indem andere Server gefragt werden, ob die Angaben eines Teilnehmers auf einem Server korrekt sind[27], festgestellt werden kann. Des Weiteren kann dieser im Namen der Teilnehmer Aktivitäten ausführen, wenn keine Verschlüsselungsmethoden genutzt werden oder nicht von dem Client selber durchgeführt werden. Ebenso können die eigenen Teilnehmer über die Aktionen anderer Teilnehmer getäuscht werden. Damit die Teilnehmer den Organisationseinheiten der Server vertrauen können, muss Fehlverhalten

[26] Hierbei ist wichtig, dass die Authentizitität der Kommunikationspartner gesichert wird, damit ein Server nicht imitiert werden kann.

[27] Beispielsweise kann angefragt werden, ob die soziale Beziehung zu einem Teilnehmer existiert.

beobachtbar sein und kommuniziert werden. Gegebenenfalls bietet es sich an, Kontrollen von Nachrichten durchzuführen, indem beispielweise Nachrichten auf zwei unterschiedlichen Wegen übertragen werden[28] oder ein Teilnehmer mehrere Server von verschiedenen Organisationseinheiten verwendet. Versucht der Client als Angreifer zu agieren, so kann er in dieser Dezentralisierungsform keine Fremdaktionen von sich oder anderen Teilnehmern vortäuschen, da alle Aktionen von dem Server registriert werden. Dies wird erst durch Verschlüsselung der Aktionsdaten möglich, da der Server keine Aussagen mehr über getätigte Aktionen treffen kann. Damit andere Teilnehmer sich trotzdem von der Authentizität der Daten überzeugen können, ist es eine Möglichkeit, Kontrollen durchzuführen, indem andere Teilnehmer befragt werden, ob eine Aktion durchgeführt wurde, was allerdings auch verwendet werden kann, um an vertrauliche Informationen zu gelangen und somit die Privatsphäre zu verletzen. Eine andere Möglichkeit ist es, jede Aktion von den anderen betroffenen Teilnehmern zusammen mit einer digitalen Signatur quittieren zu lassen. Somit lässt sich auch das Fehlverhalten eines bösartigen Servers aufdecken. Dies führt jedoch zu mehr Aufwand durch weitere Übertragungen und setzt voraus, dass eine oder mehrere Möglichkeiten existieren, mit der ein Teilnehmer die Schlüssel der anderen Teilnehmer beziehen kann. Zur Übertragung der Schlüssel sollten nicht die Server der Teilnehmer verwendet werden, da sonst ein Man-in-the-middle-Angriff möglich wird. Des Weiteren ist zu beachten, dass jeder Teilnehmer nur den Teil der Daten überprüfen kann, den ein anderer Teilnehmer von sich preisgibt.

Accountdaten können von dem jeweiligen Server kontrolliert und sichergestellt werden. Da die Kontrollen allerdings durch verschiedene Organisationseinheiten ausgeführt werden, kann nicht garantiert werden, dass jede Organisationseinheit die Kontrollen mit den gleichen Standards durchführt. Ein Teilnehmer, der seinen eigenen Server betreibt, kann somit auch den Kontrollen entgehen und beispielsweise seine Metadaten, wie das Registrierungsdatum, selbst festlegen. Um dem entgegenzuwirken, kann Vertrauen für eine Organisationseinheit zum Einsatz kommen oder es werden Dienste verwendet, die die Kontrollen übernehmen und somit Sicherheit für die Teilnehmer garantieren (siehe Abschnitt 6.4). Für die abgeleiteten und aggregierten Daten können Informationen für die eigenen Teilnehmer und für solche, deren Daten aufgrund von Interaktionen gesammelt werden konnten, mit einbezogen werden. Hierbei existiert die Möglichkeit, dass die Server untereinander Daten austauschen oder durchsuchbar machen. Dies führt allerdings zu Problemen mit der Privatsphäre, wie in sozialen Netzwerken mit zentralen Organisationseinheiten,

[28] Beispielsweise zusätzlich über ein P2P-Netzwerk.

wenn die Daten nicht anonymisiert werden. Somit ist immer nur ein beschränkter Überblick über das soziale Netzwerk möglich, vorausgesetzt es existiert keine Organisationseinheit, die einen großen Teil der Accounts der Teilnehmer beherbergt. Die Teilnehmer können ebenfalls, wenn die Aktionsdaten verschlüsselt werden, aggregierte und abgeleitete Informationen über sich selbst für andere Teilnehmer freigeben. Trotzdem wird so nur eine Teilmenge ersichtlich, da die Daten über viele Server aggregiert werden müssen, wenn ein Überblick des Netzwerkes erforderlich ist. Außerdem ist es erforderlich, einen Beleg über angegebene Aktionen einzuholen, da ansonsten jeder Server Aktionen frei erfinden kann.

5.5 Soziale Netzwerke auf Basis von P2P-Netzwerke

In sozialen Netzwerken auf P2P-Basis wird nach Möglichkeit die Kommunikation und das Speichern von Daten ohne Server bewerkstelligt, um die Nachteile einer Organisationseinheit zu umgehen. Allerdings müssen dafür die Daten des sozialen Netzwerkes auf den jeweiligen Peers gespeichert werden. Da es sich bei den Peers um die Endgeräte (Computer, Tablet, Handy und weitere) der Teilnehmer handelt, sind diese im Gegensatz zu einem Server nicht dauerhaft mit dem Netzwerk verbunden. Allerdings wird in sozialen Netzwerken eine hohe Verfügbarkeit der Daten benötigt, da die Teilnehmer in der Lage sein wollen, Änderungen und Neuigkeiten zeitlich voneinander entkoppelt, zu empfangen. Dies wird über redundantes Speichern der Teilnehmerdaten auf den anderen Peers erreicht. Es existieren mehrere Varianten, um die Daten, nach der Verteilung auf das Netzwerk, wieder zu finden. Je nachdem, ob die Peers in einer bestimmten Struktur angeordnet werden oder keine Struktur verfolgen, spricht man von strukturierten und unstrukturierten P2P-Overlays. Unstrukturierte P2P-Overlays werden unter anderem für File-Sharing-Anwendungen eingesetzt [41, S. 119-124], da die Dateien meist auf mehreren Peers in der gleichen Version vorliegen und nicht verändert werden. Unstrukturierte P2P-Overlays sind effizient darin, häufig vorkommende Dateien in dem Overlay zu finden und ebenso ineffizient bei selten vorkommenden Dateien. Die Anforderungen für soziale Netzwerke unterscheiden sich allerdings von den Anforderungen des File-Sharings [21], da die Profile in dem sozialen Netzwerk (Dateien in dem Overlay) regelmäßig durch die Interaktion der Teilnehmer verändert werden und die Daten meist nicht für alle anderen Teilnehmer sichtbar sein sollen. Damit also kein unberechtigter Lese- oder Schreibzugriff erfolgt, werden die Profile, im Gegensatz zu den Dateien beim File-Sharing, verschlüsselt. Des Weiteren sind Dateien, wie Videos und Musikstücke, in

einer hoher Anzahl in einem File-Sharing-System gegeben, da die Nutzer diese selbst auf ihre Endgeräte kopieren. Dieser Aspekt trifft nicht unbedingt auf die Daten eines Teilnehmers in einem sozialen Netzwerk zu. Strukturierte Overlays ermöglichen im Vergleich zu unstrukturierten Overlays das Auffinden von Objekten mit einer Laufzeit zwischen O(log N) und O(log 1) [24, S. 226-227]. Zusätzlich eignet sich ein strukturiertes Overlay, durch das schnelle Auffinden von Objekten, zum Hinterlegen von Benachrichtigungen für einen Teilnehmer, der offline ist. Der Nachteil dabei ist, dass das Overlay durch das Betreten und Verlassen der Teilnehmer[29] neu geordnet werden muss. Des Weiteren müssen die Daten so verteilt werden, dass die Verfügbarkeit der Daten durch das Eintreten und Verlassen der Peers nicht eingeschränkt wird. Ebenso muss ein Overlay mit heterogenen Endgeräten umgehen können. Mobile Endgeräte sind teilweise nur eingeschränkt verfügbar und haben weniger Ressourcen, weshalb es von Vorteil sein kann, diese nicht direkt in einem Overlay teilnehmen zu lassen. Alternativ können diese sich zu einem Peer in dem Overlay, wie einer DHT, verbinden.

Eine Vielzahl an wissenschaftlichen Publikationen für soziale Netzwerke auf Basis eines P2P-Netzwerkes bilden ein strukturiertes Overlay, wobei DHTs häufig zum Einsatz kommen [13, 16, 20, 40, 50, 52, 66]. Die Teilnehmerdaten können dabei komplett in dem Overlay liegen. Alternativ dazu ist es auch möglich, nur die Metainformationen in dem Overlay abzulegen, anhand dessen ein Peer in dem sozialen Netzwerk, der das gesuchte Objekt beherbergt, kontaktiert werden kann. Danach können dann weitere Interaktionen außerhalb des Overlays zwischen den beiden Teilnehmer stattfinden. Auch eine Kombination aus mehreren Overlays, beispielsweise ein Overlay zum Suchen von Teilnehmern und ein Overlay zum Versenden von Nachrichten ist möglich. In dem Fall, dass die Profile vollständig im Overlay liegen, können die Interaktionen direkt über Overlays getätigt werden, so dass Kommunikation über die Modifikation der Teilnehmerdaten stattfindet. Die Peers, die die Daten beherbergen, müssen dabei nicht Eigentümer der Profile sein, welche sie beherbergen. Über die Peers wird die Suche in dem Overlay und das Übertragen der Daten an den anfragenden Teilnehmer ermöglicht. Abbildung 10 zeigt beispielhaft die Suche und die anschließende Übertragung der Daten, wobei zu beachten ist, dass die Geräte der Teilnehmer auch ein Teil des Overlays sein können. In dem zweiten Fall, bei dem nur Metadaten in dem Overlay gespeichert werden, wird das Overlay hauptsächlich zum Suchen von Objekten verwendet. Das Resultat einer Anfrage kann beispiels-

[29] Hierbei ist nicht der Registrierungsprozess oder das Löschen gemeint, sondern der Wechsel zwischen On- und Offline gehen eines Teilnehmers.

weise die IP-Adresse eines Peers beinhalten, zu dem sich dann der anfragende Peer verbinden kann (siehe Abbildung 11), wie es beispielsweise bei PeerSoN der Fall ist [13]. In dieser Form ermöglichen beide Varianten das Erhalten neuer Informationen als Pull-Verfahren, was bedeutet, dass die Teilnehmer selbst aktiv werden müssen, um über Neuigkeiten informiert zu werden. Die Verwendung des Push-Verfahren bietet den Vorteil, dass die Peers nicht stetig nach neuen Informationen anfragen müssen, sondern diese übermittelt bekommen, wenn welche vorliegen. Dies kann erreicht werden, indem die Teilnehmer direkte Verbindungen zu den anderen Teilnehmern aufbauen und die Informationen übertragen oder Verfahren nutzen, bei denen andere Teilnehmer in dem Netzwerk die Änderungen für sie publizieren. Zur Umsetzung dieser Verfahren kann das Overlay auf Push-Benachrichtigungen ausgelegt werden. Beispielsweise werden in [52] auf der Basis von DHTs Baumstrukturen gebildet, um Nachrichten zu verschicken (siehe Abbildung 12). Hierbei schließt sich ein Teilnehmer einem Baum an, um die Nachrichten zu erhalten, die durch die Baumstruktur von oben nach unten über die einzelnen Knoten geleitet werden. Alternativ dazu lassen sich auch Verfahren aus unstrukturierten P2P-Overlays verwenden, wie Gossip-Algorithmen in Cuckoo oder Random Walks. Dabei beschäftigen sich aktuelle Arbeiten [42, 48] damit, diese Verfahren mittels sozialer Overlays auf die Eigenschaften sozialer Netzwerke anzupassen.

5.5.1 Betrachtung der Auswirkungen auf die Teilnehmerdaten

Hinsichtlich der Accountdaten gibt es keine allgemein vertrauenswürdige Instanz, die Kontrollen durchführen kann. Einige Ansätze versuchen diesen Nachteil durch eine Einführung einer zentralen Organisationseinheit, welche allerdings getrennt von dem sozialen Netzwerk agiert, wieder auszugleichen. Vor- und Nachteile dieses Vorgehens werden in Abschnitt 6.4 besprochen.

Bei den Aktionsdaten werden, wenn keine direkte Verbindungen zwischen den Teilnehmern existieren, die Aktionen durch das Overlay geroutet. Allerdings erscheint es nicht möglich, die Peers in dem Overlay als vertrauenswürdige Instanzen, wie eine zentrale Organisationseinheit zu verwenden, um eine Kontrollinstanz für Aktionsdaten einzuführen. Dies liegt daran, dass zwischen den Peers ein jeweils unterschiedliches Vertrauensverhältnis vorliegt. Teilnehmer können anonym oder unbekannt für den einen Teilnehmer sein, während andere Teilnehmer in einer engen sozialen Beziehung zu diesem Teilnehmer stehen. Dafür lässt sich soziales Vertrauen verwenden, um die Beziehungen zwischen den Teilnehmern, zum Bilden eines

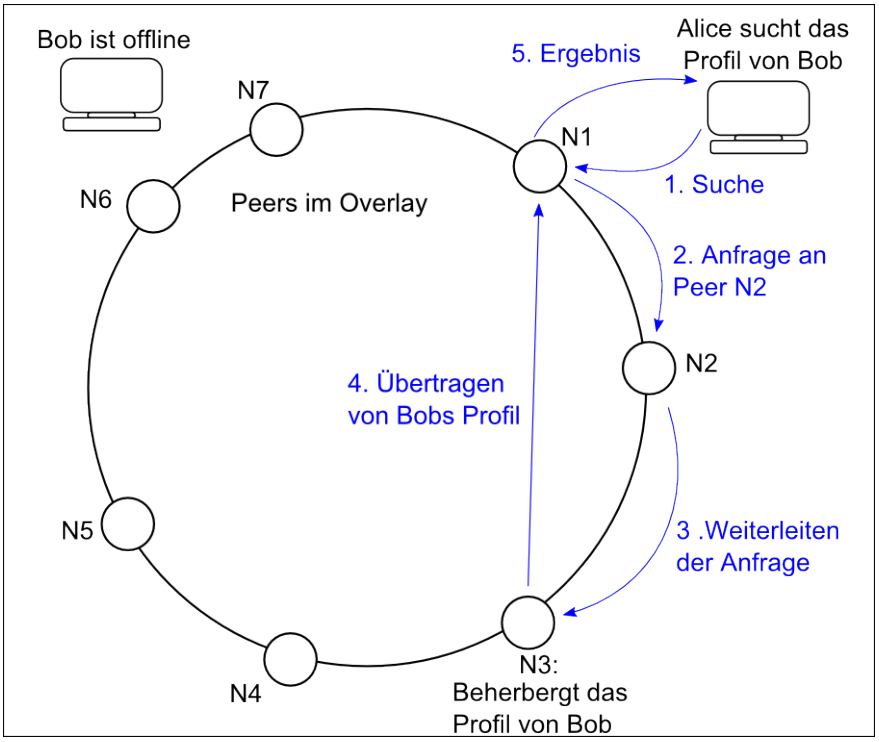

Abbildung 10: Aufruf eines Profils in einer Ring-förmigen DHT und einem simplen Suchverfahren

Overlays aus sich gegenseitig vertrauenden Teilnehmern, nutzen. Geht man davon aus, dass die Durchführung einer Aktion nicht durch vertrauenswürdige Instanzen, wie in einem sozialen Overlay gesichert wird, bietet sich hier wieder das Erbringen von Nachweisen an, um Aktionsdaten auf Durchführung überprüfen zu können. Um einen Überblick der Eigenaktionen bzw. Fremdaktionen, wie die Anzahl der Aufrufe eines Profils zu erhalten, müssen die Daten aller Teilnehmer, die die Daten des Profils beherbergen, gesammelt und zusammengeführt werden. Dies kommt dadurch zustande, dass die Daten nicht bei einem Teilnehmer gespeichert, sondern über mehrere Teilnehmer redundant verteilt werden. Somit ist es möglich, dass das Abrufen der Daten eines Accounts zur Interaktion mit verschiedenen Peers führen kann, die jeweils einen Teil der benötigten Daten halten. Dagegen führen Fremdaktionen, die die Zustimmung eines Teilnehmers benötigen, wie etwa eine Freundschaftsanfrage, dazu, dass der Teilnehmer zu dem Account in jedem Fall informiert werden muss, damit die Aktion erfolgreich abgeschlossen werden kann und somit der Teilnehmer genau sagen kann, ob diese Aktion stattgefunden hat. Die Schwierigkeit einen Überblick der Zugriffe auf einen Account zu sammeln, wirken sich wiederrum auf

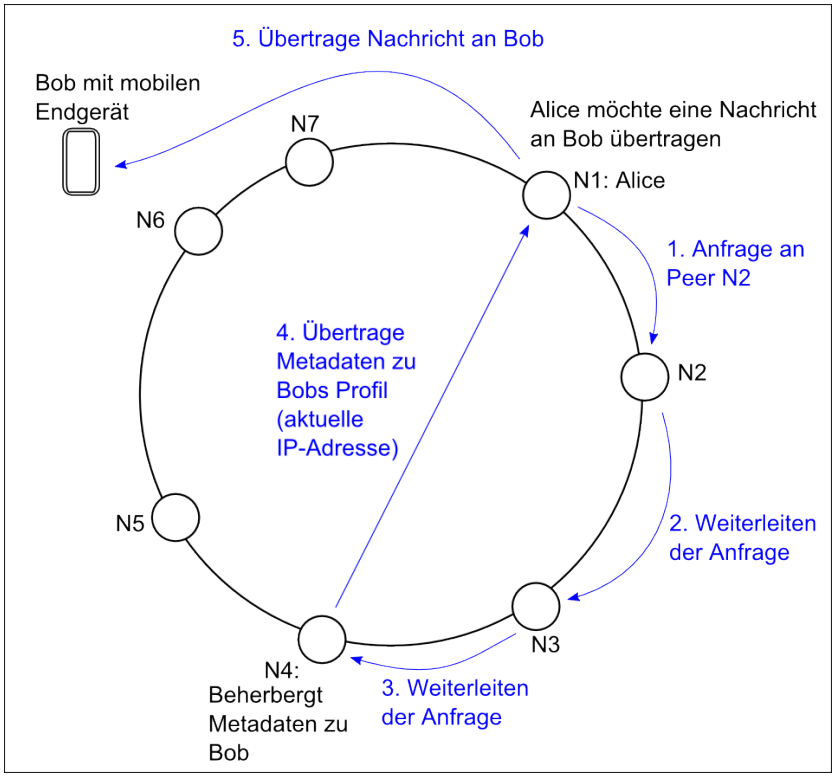

Abbildung 11: Übertragen einer Nachricht mit vorheriger Suche in einem Ringförmigen DHT und anschließender direkter Übertragung nach dem Prinzip aus [13]

abgeleitete und aggregierte Informationen aus, so dass ein Teilnehmer diese Informationen ermitteln kann, wenn sie ihn direkt betreffen und für ihn sichtbar sind. Bei den Inhalten der Aktionen werden kryptographische Verfahren eingesetzt, damit der Schutz der Privatsphäre gewährleistet wird. Somit sind die Inhalte nur für berechtigte Teilnehmer sichtbar. Der Peer, der die Daten beherbergt, kann gegebenenfalls anhand der Zugriffsberechtigungen erkennen, wer Zugriff auf die Daten hat. Dies ist allerdings von den Verfahren abhängig und wird in Abschnitt 6.1 betrachtet. Ebenso können Teilnehmer auf dem Pfad zwischen den zwei Teilnehmern einer Kommunikation sowie externe Angreifer, welche das Netzwerk abhören, beobachten welche Teilnehmer miteinander kommunizieren. Es können also gegebenenfalls Metadaten über die Kommunikation abgeleitet werden, was zu einer Verletzung der Privatsphäre führen kann. Eine Lösung zu diesem Problem wird mit Safebook [20] vorgestellt. Hierbei wird ein Overlay aus den sozialen Kontakten eines Teilnehmers gebildet, um die Metadaten der Kommunikation zu verbergen. Die Kontakte des Teilnehmers

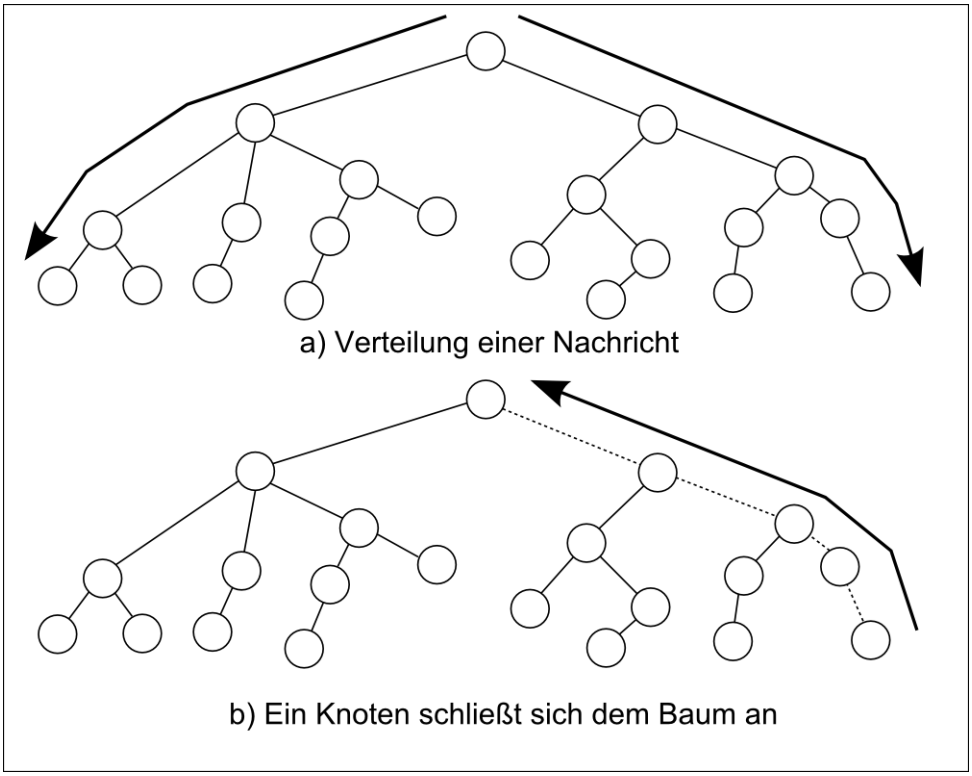

Abbildung 12: Ein Overlay zum Versenden von Push-Benachrichtigungen. Modifiziert aus [52]

werden als konzentrische Kreise (Matryoshka) um den Teilnehmer angeordnet, wie in Abbildung 13 zu sehen ist. Die Kommunikation zu einem Teilnehmer durchläuft den Matryoshka, wobei jeder Teilnehmer die Adresse des Absenders überschreibt, womit sich für andere Peers oder einen Angreifer nicht mehr genau ableiten lässt, wer der Autor der Nachricht ist. In anderen Systemen, die auf direkte Kommunikation setzen, sind die Metadaten, wie die IP-Adresse, öffentlich zugänglich, damit direkte Verbindungen zwischen den Peers möglich sind. Nach dem Abrufen der IP-Adresse aus dem Overlay, ist es für einen Dritten nur noch über das Abhören des Netzwerkes möglich, Informationen über die Kommunikation zu erhalten. Wie Paul et al. berichten, ist dies auch ein weiterer Unterschied zu der Verwendung einer zentralen Organisationseinheit. Hierbei sind alle Nachrichten immer an die Server der Organisationseinheit gerichtet, so dass anhand der Adresse ein Angreifer nicht sagen kann, an wen die Nachricht gerichtet ist.

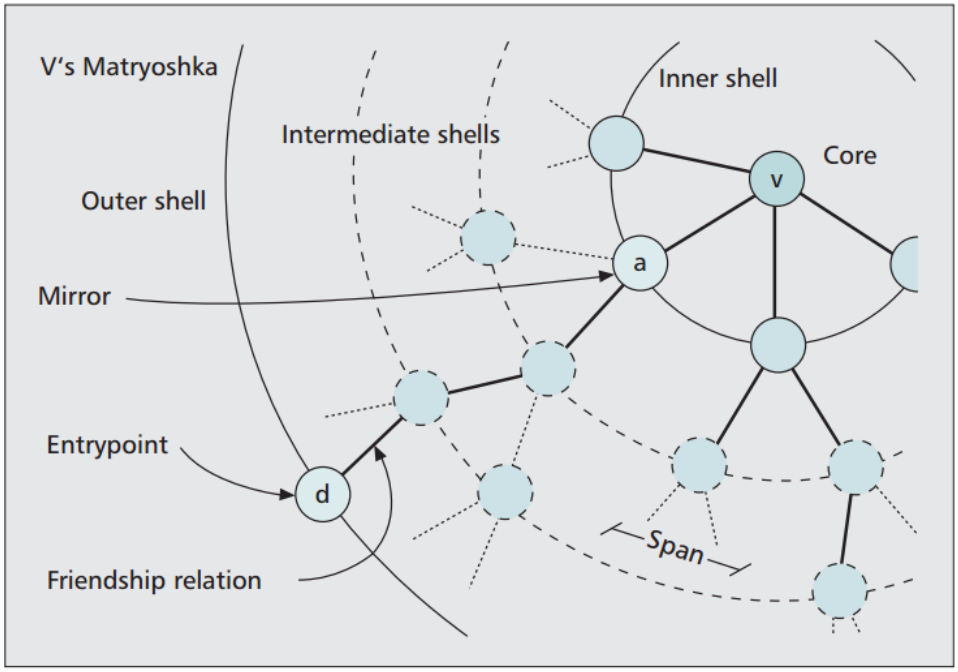

Abbildung 13: Struktur eines Matryoshka aus [20]

5.5.2 Sicherheitsmaßnahmen in strukturierten Overlays

Strukturierte Overlays bieten die Möglichkeit zum Speichern, Suchen und Verteilen von Objekten. Allerdings können bösartige Teilnehmer innerhalb des Overlays Objekte unterschlagen, damit diese nicht gefunden oder verteilt werden können. Ebenso kann ein bösartiger Teilnehmer falsche Nachrichten auf eine Suchanfrage liefern oder das Overlay stören, indem beispielsweise Änderungen an die Routingtabellen der anderen Teilnehmer kommuniziert werden, die zu falschen Routen oder DDoS-Angriffen führen. Eine andere Möglichkeit ist, dass ein Angreifer versucht, in den Zuständigkeitsbereich eines Objektes zu gelangen, sodass er bestimmte Objekte aus dem Overlay entfernen oder korrumpieren kann. Damit der Angreifer in die richtige Position kommen kann, um als Peer in dem Overlay die Zuständigkeit zum Beherbergen eines bestimmten Objektes zu erhalten, können Schwächen in der Vergabe der ID genutzt werden. Wie in Abschnitt 5.3 beschrieben, ist die ID ausschlaggebend dafür, in welchem Bereich ein Peer in dem DHT zuständig ist. Gelingt es dem Angreifer eine ID nach seinen Bedürfnissen zu erhalten, kann er somit in den Zuständigkeitsbereich für ein Objekt gelangen oder in die Routingtabelle eines anderen Teilnehmers [14, S. 326]. Dies kann gegebenenfalls auch über Sybils erreicht

werden, da der Angreifer mittels mehrerer Identitäten versucht, die Chancen auf eine günstige Position zu erhöhen oder an mehreren Stellen angreifen kann, indem beispielsweise Nachrichten unterschlagen werden.

Gegen eine Vielzahl der Angriffe helfen kryptographische Verfahren, weil die Rückgabe falscher Objekte erkannt wird und Manipulationen der Objekte nicht möglich sind, da ein Angreifer kein Objekt mit einer entsprechenden Signatur erstellen kann. Damit Objekte durch das unberechtigte Entfernen nicht verloren gehen, kommen Verfahren zur Replikation zum Tragen. Ein Angreifer kann aber allerdings weiterhin falsche Objekte zurückgeben, indem ältere Zustände eines Objektes verwendet werden (ähnlich zu einem Reply-Angriff). Hierfür ist es erforderlich, dass das Routen in dem Overlay funktioniert, damit aktuellere Zustände des Objektes gefunden werden können. Für das korrekte Routen gilt es, zum einen die Anwesenheit von Sybils zu minimieren und zum anderen Verfahren zu verwenden, die Objekte mit einer hohen Wahrscheinlichkeit finden [61]. Um dies zu erreichen werden unter anderem. Replikationen und redundante Routingprozesse verwendet. Ebenso kann auch soziales Vertrauen angewendet werden, um die Daten über möglichst vertrauenswürdige Teilnehmer zu leiten. Zusätzlich zu dem sicheren Routen, müssen die Verfahren zur Vergabe von IDs gegenüber Angriffen gesichert werden. Hierbei bieten sich zentrale Instanzen an, die die IDs zufällig vergeben. Andere Verfahren zwingen die Peers nach einiger Zeit zum erneuten Eintritt in das Overlay oder speichern die IP-Adressen der Peers in dem Overlay, damit keine IP-Adresse mehrmals vorkommt.

Detailliertere Beschreibungen zur Bekämpfung von Angriffen in Overlays können der Literatur [14, 18, 61] entnommen werden. Allerdings werden die Verfahren zur Bekämpfung von Sybils in Abschnitt 6.4 vorgestellt, da diese nicht nur für das Routen innerhalb strukturierter Overlays ein Problem darstellen, sondern auch die Authentizität von Teilnehmerdaten verletzen können. Ebenso wird auf kryptographische Verfahren in 6.1 eingegangen, da diese übergreifend für alle Dezentralisierungsformen relevant sind.

5.6 Zusammenfassung

Ziel dieses Kapitels war es, die Auswirkungen auf die Teilnehmerdaten durch die Dezentralisierung von sozialen Netzwerken zu analysieren und Bereiche zu identifizieren, die für die Authentizität und Integrität der Teilnehmerdaten relevant sind. Hinsichtlich der Teilnehmerdaten lässt sich festhalten, dass jegliche Form von Dezentralisierung dazu beiträgt, dass ein Teil der aggregierten und abgeleiteten Daten

nur durch die Kooperation der Teilnehmer und der Organisationseinheiten erfasst werden können. Eine zentrale Organisationseinheit bringt hierbei den Vorteil, dass immer noch eine Vielzahl an Daten erfasst werden, bis auf Eigenaktionen und Fremdaktionen, die keine Indizien auf die Durchführung erlauben. Bei den Aktionsdaten kann eine Organisationseinheiten die Durchführung einer Aktion bezeugen, wenn die Kommunikation über die Server der Organisationeinheit stattfindet. Dafür muss allerdings jede an der Kommunikation beteiligte Organisationseinheit vertrauenswürdig sein, was beispielsweise in Infrastrukturen, bei denen jeder Teilnehmer einen eigenen Server stellen kann, nur bedingt gegeben ist. Der Umfang an Informationen, die eine Organisationseinheit bei den Aktionsdaten sammeln kann, lässt sich mittels kryptographischer Verfahren begrenzen. Je nachdem, welche Anteile der Aktionen verschlüsselt werden, bleiben Teile der Metainformationen, die Art der Aktion oder die Inhalte für die Organisationseinheit verborgen. Zur Sicherungen der Accountdaten lassen sich die Kontrollen von zentralen Organisationseinheiten durchführen. Diese sind allerdings gegebenenfalls sehr aufwendig (siehe Abschnitt 4.3.1). Ein Überblick, wie sich die Dezentralisierung auf die Teilnehmerdaten auswirkt und wie die Daten in den jeweiligen Formen gesichert werden, ist in den Tabellen 6, 7, 8 und 9 dargestellt.

Hinsichtlich der Bereiche, in denen Maßnahmen durchgeführt werden müssen, zeigt sich dass kryptographische Verfahren häufig zum Schutz der Integrität, Privatsphäre und zur Überprüfung der Urheberschaft verwendet werden. Dabei muss allerdings sichergestellt werden, dass die Schlüssel authentisch bei den Teilnehmern vorliegen. Die Durchführung und die Authentizität einer Aktion wird über das Vertrauen in eine oder mehrere Organisationseinheiten gesichert. Für den Fall, dass keine vertrauenswürdige Instanz an der Kommunikation beteiligt ist, werden Nachweise oder andere Verfahren benötigt, um festzustellen, ob eine Aktion wirklich stattgefunden hat und von einer Organisationseinheit oder einem Teilnehmer nicht nur vorgegeben werden. Des Weiteren werden in jeweiligen Dezentralisierungsformen Verfahren benötigt, um aggregierte und abgeleitete Daten zu erheben, wenn es möglich sein soll, hieraus beispielsweise Erkenntnisse für die Glaubwürdigkeit anderer Teilnehmer gewinnen zu können. Aus den vorher beschriebenen Kapiteln und der Sicherheitsanalyse zu sozialen Netzwerken auf Basis von P2P-Netzwerken gilt es zudem den Anteil an Sybils, wenn möglich, zu begrenzen.

6 Mechanismen und Bewertung

In diesem Kapitel geht es darum, einzelne Verfahren zum Schutz der Authentizität und Integrität von Teilnehmerdaten zu betrachten und entsprechend zu bewerten. Den Rahmen für die Auswahl der Verfahren geben die vorherigen Kapitel dieser Arbeit. Somit ergibt sich aus der Betrachtung der Angriffe, dass unter anderem Mechanismen zur Authentifizierung der Teilnehmer und Zugriffskontrollen relevant sind. Durch die Analyse der Teilnehmerdaten und welche Auswirkung die Dezentralisierung auf diese Daten hat, ergibt sich ein Bedarf nach Mechanismen, die die Durchführung einer Aktion sicherstellen können. Des Weiteren gilt es auch Angriffe durch Sybilaccounts zu berücksichtigen. Innerhalb dieses Kapitels werden die verschiedene Mechanismen für diese Bereiche vorgestellt. Dabei wird davon ausgegangen, dass es sich bei der Infrastruktur der sozialen Netzwerke, um dezentrale Server oder ein P2P-Netzwerk handelt. Die Infrastruktur mit einer zentralen Organisationseinheit mit Unterstützung durch ein P2P-Netzwerk wird hier nicht weiter vertieft, da in dieser Dezentralisierungsform entweder die gleichen Sicherheitsanforderungen, wie in einem sozialen Netzwerk auf Basis eines P2P-Netzwerkes bestehen oder auf die zentrale Organisationseinheit zurückgegriffen werden kann.

6.1 Zugriffskontrollen und Kryptographie

Bei den Verfahren, die innerhalb der Analyse der Dezentralisierungsformen vorgestellt wurden, wurden kryptographische Verfahren häufig verwendet, um die Integrität, Authentizität und Vertraulichkeit der Teilnehmerdaten in sozialen Netzwerken zu schützen. In diesem Abschnitt wird analysiert, wie sich die einzelnen kryptographischen Verfahren einsetzen lassen, um die Einhaltung der Schutzziele zu wahren.

Da ein soziales Netzwerk durch die Teilnehmerdaten abgebildet wird, werden unter anderem die Profile, private Nachrichten, Pinnwandeinträge und Informationen über die Beziehungen der Teilnehmer auf nicht vertrauenswürdigen Instanzen abgelegt oder über diese übertragen. Damit nur berechtigte Teilnehmer unter den Bedingungen einer dezentralen Umgebung mit nicht vertrauenswürdigen Teilnehmern auf die Daten zugreifen können, lassen sich kryptographische Verfahren einsetzen, um eine Zugriffskontrolle umzusetzen. Die Zugriffskontrolle besteht aus Berechtigungen für Lese- und Schreibzugriffe, die für einzelne Teilnehmer oder Gruppen von Teilnehmern vergeben werden können, um beispielsweise auch Einträge verschiedener Teilnehmer an einer Pinnwand abbilden zu können. Die Zugriffsberechtigung, die an eine einzelne Person oder an die Personen einer Gruppe vergeben wurde, muss

auch wieder entzogen werden können. Ein Teilnehmer, der eine Anfrage stellt, ein Objekt zu lesen, hinzuzufügen oder zu verändern, muss sich entsprechend gegenüber einer Instanz, die die Daten hält, authentifizieren können. Dies kann beispielsweise erforderlich sein, um einen Kommentar für einen anderen Teilnehmer hinterlassen zu können. Dabei muss von der Instanz, die die Daten hält, geprüft werden, dass keine anderen Daten von dem Teilnehmer durch die Aktion korrumpiert werden. Dabei gilt es, auch die Privatsphäre zu schützen, damit nicht nur unberechtigten Teilnehmern der Zugriff verwehrt bleibt, sondern auch die Instanzen, die die Daten halten oder übertragen, keine Informationen über die Teilnehmer sammeln können. Der lesende Zugriff kann auch alternativ darüber gesichert werden, dass der Teilnehmer das Objekt erhält, dieses aber nicht entschlüsseln kann.

Um Zugriffskontrollen dieser Art umzusetzen, bieten sich verschiedene Verfahren an. Bei lesenden Zugriffen ist zu unterscheiden, ob es sich dabei um Kommunikation nach dem Push- oder Pull-Paradigma handelt. Bei dem Push-Paradigma verfügt die Instanz, die gerade die Daten hält, Informationen darüber, an wen sie die Daten übertragen soll, während bei dem Pull-Paradigma die Teilnehmer selber Anfragen stellen und somit die Instanz nicht weiß, ob es sich hierbei um einen berechtigten Zugriff handelt. Im weiteren Verlauf werden zuerst Umsetzungen mittels asymmetrischer und symmetrischer Verfahren angeführt und danach auf Attribute-based Encryption (ABE) eingegangen.

6.1.1 Asymmetrische und symmetrische Verschlüsselung

Eine bekannte Methode um die Integrität und die Authentizität von Daten bei der Übertragung bzw. Speicherung zu schützen, ist asymmetrische Verschlüsselung. Hierbei hat jeder Teilnehmer einen privaten und einen öffentlichen Schlüssel. Der öffentliche Schlüssel muss für andere Teilnehmer zugänglich sein und der private Schlüssel darf nur dem entsprechenden Teilnehmer selbst bekannt sein. Daten, die mit dem privaten Schlüssel verschlüsselt werden, können von allen Teilnehmern mit dem dazugehörigen öffentlichen Schlüssel entschlüsselt werden. Allerdings ist nur der Teilnehmer, der über den privaten Schlüssel verfügt, in der Lage, die Daten so zu verschlüsseln, dass sie sich mit dem öffentlichen Schlüssel entschlüsseln lassen. Somit wird die Authentizität des Absenders sichergestellt, wobei man hier von einer Signatur spricht. Andersherum können die Teilnehmer mit dem öffentlichen Schlüssel eine Nachricht so verschlüsseln, dass kein anderer Teilnehmer, außer dem Teilnehmer mit dem dazugehörigen privaten Schlüssel, die Nachricht entschlüsseln kann. Somit lässt

sich die Vertraulichkeit der Nachricht sichern. Die Integrität wird dabei allerdings nur eingeschränkt gesichert, da ein Angreifer nicht in der Lage ist, eine Nachricht zu erstellen oder so zu verändern, dass die Entschlüsselung einen sinnvollen Klartext ergeben sollte. Allerdings hat der Empfänger somit keinen klaren Beweis, dass die Nachricht verändert wurde. Um die Integrität zu sichern, bietet sich deshalb die Verwendungen von digitalen Signaturen an (siehe Abschnitt 6.1.3). Verschlüsselt ein Teilnehmer eine Nachricht mit dem öffentlichen Schlüssel eines anderen Teilnehmers und signiert die Nachricht danach durch die Verschlüsselung mit seinem privaten Schlüssel, so lassen sich die Authentizität und Vertraulichkeit der Nachricht sichern. Dabei muss sichergestellt werden, dass die Kommunikationsteilnehmer über den korrekten öffentlichen Schlüssel des jeweiligen Kommunikationspartners verfügen, da ansonsten ein Angreifer auf dem Kommunikationsweg gegebenenfalls die Nachrichten verändern, einsehen oder im Namen eines anderen Teilnehmers Nachrichten versenden kann. Die symmetrische Verschlüsselung ist von den Operationen her weniger rechenintensiv als asymmetrische Verschlüsselungsverfahren, bietet dafür allerdings nur die Möglichkeit die Vertraulichkeit herzustellen[30]. Hierbei benutzen die Kommunikationsteilnehmer einen gemeinsamen geheimen Schlüssel, um die Nachrichten zu verschlüsseln beziehungsweise zu entschlüsseln.

Damit nun ein Teilnehmer andere Teilnehmer mittels Nachrichten über Änderungen in seinem Profil informieren (beispielsweise ein Pinnwandeintrag) oder die Daten für den späteren Ablauf hinterlegen kann, bietet sich die Signierung der Nachricht zum Herstellen von Authentizität an. Des Weiteren wird die Nachricht so verschlüsselt, dass nur berechtigte Teilnehmer diese lesen können. Da bei asymmetrischen Verfahren die Verschlüsselung mit den privaten Schlüssel des jeweiligen anderen Teilnehmers erfolgt, bietet es sich an, bei 1-zu-n-Kommunikationen, wie Pinnwandeinträgen, einen Schlüssel mit einer Gruppe zu teilen, damit nicht für jeden Teilnehmer der Gruppe eine Nachricht verschlüsselt und signiert werden muss. Hierbei werden symmetrische Verschlüsselungsverfahren bevorzugt, da sie weniger Rechenkapazität benötigen. Mittels eines symmetrischen Schlüssel können auch andere Teilnehmer in dieser Gruppe Nachrichten erzeugen. Damit die Authentizität gewährleistet ist, kann die Nachricht nach der Verschlüsselung mit dem symmetrischen Verfahren, mit einem asymmetrischen Verfahren signiert werden. Es ist allerdings vorher notwendig, dass die Teilnehmer den symmetrischen Schlüssel erhalten, wozu

[30] Es sei denn, die beiden Kommunikationspartner sind die einzigen, die diesen Schlüssel verwenden, dann kann ein Teilnehmer davon ausgehen, dass die Nachricht von dem jeweils anderen Teilnehmer stammt. Dabei sind allerdings weiterhin Replay-Attacken möglich.

der Teilnehmer an alle Teilnehmer der Gruppe den Schlüssel verteilt, welcher zuvor mit einem asymmetrischen Verfahren verschlüsselt wird, damit nur die berechtigten Teilnehmer die Nachricht entschlüsseln können. Dies muss jedes Mal gemacht werden, wenn eine neue Gruppe erstellt wird, der Gruppenschlüssel sich ändert oder einem Teilnehmer der Zugriff verwehrt werden soll. Da dies je nach Anzahl der betroffenen Teilnehmer zu höherem Rechenaufwand führen kann, lässt sich diese Aufgabe auch an andere Teilnehmer, wie den Peers in einem P2P-Netzwerk, delegieren [52]. Dabei müssen die Teilnehmer, die den privaten Schlüssel weitergeben, darüber informiert werden, welcher Teilnehmer diesen erhalten darf. Eine Zugriffskontrolle für Gruppen mittels symmetrischer Verschlüsselung hat allerdings den Nachteil, dass Und-Verknüpfungen für Gruppenberechtigungen nicht ausreichend umgesetzt werden können. Wie in [5] beschrieben, kann eine Nachricht beispielsweise für eine Gruppe *Kollegen* oder *Freunde* freigegeben werden, indem die Nachricht zwei mal versendet beziehungsweise gespeichert, aber jeweils nur einer der Gruppenschlüssel verwendet wird. Wird aber eine Nachricht mittels der beiden Gruppenschlüssel verschlüsselt, so dass ein Teilnehmer, der in der Gruppe *Kollegen* und *Freunde* ist, Zugriff haben soll, können Mitglieder, die jeweils in einer der beiden Gruppen sind, kooperieren und die Nachricht über den Austausch der Schlüssel entschlüsseln. Ein weiterer Aspekt ergibt sich, wenn die Nachricht nicht direkt, sondern auf einem Server oder in einer DHT hinterlegt wird. Es empfiehlt sich bei sozialen Netzwerken, die Wert auf die Privatsphäre legen, nicht das komplette Profil als ein Objekt, wie in [16], abzuspeichern. Dies führt dazu, dass keine feingranulare Zugriffskontrolle möglich ist, da ein Teilnehmer, der das Profil eines anderen Teilnehmers abfragt, alle Daten des Teilnehmers entschlüsseln muss. Ebenso muss immer das komplette Profil abgerufen werden. Als Alternative dazu kann das Profil aus vielen Objekten zusammengesetzt werden[31], was zu dem Nachteil führt, dass möglicherweise mehrere Zugriffe erfolgen müssen, bis alle relevanten Daten abgerufen wurden. Auch hierbei sind die Daten entsprechend zu verschlüsseln, damit der Peer oder Server, der die Daten hält, diese nicht einsehen kann. Ebenso wie die Teilnehmer, die keine Berechtigung zum Abrufen der haben.

Ein anderer Ansatz ist das Verwenden von Zugriffslisten, wie in [60] beschrieben. Hierbei vergeben die Teilnehmer Nachweise an andere Teilnehmer über eine soziale Beziehung mit einer entsprechenden digitalen Signatur. Eine Instanz, die die Daten hält, kann mittels einer Zugriffsliste überprüfen, ob ein anfragender Teilnehmer berechtigt ist, auf die Daten zu zugreifen. Hierfür werden die Berechtigungen

[31] Beispielsweise kann eine Nachricht aus einem Objekt bestehen

zusammen mit den öffentlichen Schlüssel der Teilnehmer für ein Objekt abgelegt. Mittels eines Challenge-Response-Verfahrens kann dann überprüft werden, ob dieser Teilnehmer auch über den privaten Schlüssel verfügt. Damit ist eine feingranulare Zugriffskontrolle möglich, da beispielsweise ein Teilnehmer auch schreibenden Zugriff auf ein gemeinsames Objekt erhalten kann, während ein anderer nur lesenden Zugriff hat[32]. Des Weiteren können Zugriffe entzogen werden, indem Teilnehmer über die Zugriffslisten ausgeschlossen werden oder ein Nachweis über eine Beziehung mit einem Ablaufdatum versehen wird. Ebenso ist es möglich, allen Teilnehmer einen neuen Schlüssel zu übertragen, die diese Beziehung haben. Dies führt allerdings zu dem bereits oben beschriebenen Aufwand, den neuen Schlüssel zu verteilen. Der Nachteil an Zugriffslisten ist, dass ein Teilnehmer und dessen Zugriffsrechte für die Instanz, die die Daten hält, anhand des öffentlichen Schlüssels sichtbar wird. Außerdem muss die Instanz vertrauenswürdig sein, sollten die Daten unverschlüsselt gespeichert werden. Zusätzlich gilt es zu beachten, dass wenn ein neuer Schlüssel an eine Gruppe übertragen wird, um einen Teilnehmer auszuschließen, der ausgeschlossene Teilnehmer weiterhin auf alte Objekte mit seinem Schlüssel zugreifen. Um dies zu verhindern, müssen auch alle bereits bestehenden Daten mit dem neuen Schlüssel verschlüsselt werden. Alternativ lässt sich dies auch über die Zugriffslisten abbilden, wenn man davon ausgehen kann, dass die Instanzen die Zugriffslisten befolgen.

6.1.2 Attribute-based Encryption

Eine weitere Alternative zur Umsetzung von Zugriffskontrollen ist die Verwendung von ABE in Kombination mit den vorher beschriebenen Verfahren. ABE ist wesentlich langsamer als asymmetrische Verschlüsselungsverfahren wie RSA, ermöglicht dafür einige Vereinfachungen, um Zugriffskontrollen für Gruppen zu realisieren [5]. Die Freigaben für ein Objekt werden mittels logischer Operatoren[33] verknüpft. Dabei ist es nicht mehr möglich, dass Zugriffe, die eine Und-Verknüpfung verwenden, durch den Austausch der zwei einzelnen Schlüssel ausgehebelt werden können. Eine weitere Vereinfachung dabei ist, dass alle Verknüpfungen von Zugriffsgruppen in einer einzigen Verschlüsselungsoperation umgesetzt werden können, statt wie in den vorher genannten Verfahren, bei denen für jede Verknüpfung mit einem anderen Schlüssel verschlüsselt werden muss. Für den Zugriff auf ein Objekt erhält jeder

[32] In einem sozialen Netzwerk könnte dies beispielsweise der Beitrag eines Teilnehmers auf einer Pinnwand eines anderen Teilnehmers sein. Somit dürfen Teilnehmer, die eine soziale Verbindung zu dem Verfasser des Beitrages haben, diesen Beitrag sehen, aber nicht selber kommentieren, da sie nicht mit dem Besitzer des Pinnwandeintrages befreundet sind.

[33] In diesem Fall werden hier drunter eine Und- beziehungsweise Oder-Verknüpfungen verstanden.

Teilnehmer einen privaten Schlüssel von dem Teilnehmer, der die Berechtigung einrichtet. Der private Schlüssel wird dafür von dem Teilnehmer, der die Berechtigung vergibt, mittels eines Hauptschlüssels und den dazugehörigen Attributen generiert. Zur Verteilung der Schlüssel werden, wie schon bei der Verteilung der symmetrischen Schlüssel, öffentliche Schlüssel der anderen Teilnehmer verwendet. Hierbei ergibt sich ein weiterer Vorteil, da jeder Teilnehmer, der den Schlüssel eines Teilnehmers kennt, der eine Gruppe eingerichtet hat, Nachrichten an die Gruppe verfassen kann.

Ein Beispiel für ein System, welches mit ABE arbeitet, ist Persona [5]. Hierbei sind Speicherdienste vorgesehen, bei denen ein Teilnehmer seinen persönlichen Speicherbereich hat. Diesen kann der Teilnehmer auch nutzen, damit andere Teilnehmer die erstellten privaten Schlüssel abrufen können. Damit andere Teilnehmer ein Objekt in diesen persönlichen Speicher ablegen können, wie etwa einen Pinnwandeintrag, werden Zugriffslisten mit den öffentlichen Schlüsseln der berechtigten Teilnehmer verwendet. Beim Zurückziehen einer Berechtigung für einen Teilnehmer einer Gruppe, müssen alle Teilnehmer der Gruppe einen neuen Schlüssel erhalten. Dieser Aspekt und dass der öffentliche Schlüssel Aufschluss über die Berechtigungen der Teilnehmer gibt, wird in Decent [40] adressiert. Bei Decent werden die Objekte in einem P2P-Netzwerk mit einer DHT gespeichert. Auch hier kommt ABE für die Zugriffskontrolle zum Einsatz. Damit ein Objekt bearbeitet werden kann, besitzt jedes Objekt einen unverschlüsselten Eintrag, der einen öffentlichen Schlüssel für den Peer, der die Daten hält, beinhaltet. Mit diesem öffentlichen Schlüssel kann der Peer überprüfen, ob der Zugriff berechtigt ist, indem ein Challenge-Response-Verfahren verwendet wird. Der öffentliche Schlüssel ist hierbei ein anderer, als der Schlüssel, der mit der Identität eines Teilnehmers verbunden ist. Somit kann die Identität des Teilnehmers vor dem Peer, der die Daten hält, verborgen bleiben. Für Teilnehmer ohne eine Berechtigung ist es somit nicht möglich, Operationen, wie Überschreiben oder Löschen, an einem Objekt durchzuführen, da ihnen der öffentliche Schlüssel fehlt. Der Peer in dem DHT, der ein Objekt hält, kann allerdings Objekte löschen oder ein altes Objekt, statt des aktuellen Objekts, auf eine Anfrage zurück geben. Das Löschen eines Objektes stellt kein Problem dar, solange ein Peer existiert, der durch die Replikation in dem DHT noch ein korrektes Objekt beherbergt [40]. Des Weiteren werden Metadaten verwendet, die die Version eines Objektes angeben, damit die aktuellste Version in dem DHT gefunden werden kann, unter der Voraussetzung, dass das korrekte Routen funktioniert. Für das Entziehen von Zugriffsrechten verwenden die Autoren eine Modifikation des Verfahrens aus [39]. Dabei wird der

Chiffrentext zu einem Teil von einem Proxy[34] entschlüsselt, mit dem Teilnehmer den restlichen Text entschlüsseln kann. Soll dem Teilnehmer die Berechtigung entzogen werden, so wird dies über den Schlüssel, den der Proxy zum Entschlüsseln verwendet, abgebildet, sodass es dem Teilnehmer nicht mehr möglich ist, den Chiffrentext zu entschlüsseln. Somit müssen alle bestehenden Dateien nicht neu verschlüsselt, sondern nur der Schlüssel des Proxys ausgetauscht werden. Der Nachteil hierbei ist, dass es sich bei einem Proxy um eine vertrauenswürdige Instanz handelt, die auch entsprechend verfügbar sein muss.

Sowohl Persona als auch Decent versuchen den Einsatz von ABE aufgrund der teueren Operationen gering zu halten. Die Evaluation in [40] zeigt, dass es bis zu mehrere 100 Sekunden dauern kann, um das Profil eines Teilnehmers abzurufen. Die Autoren korrigieren diese Schwachstelle in einer weiteren Arbeit [50], wobei die Änderungen auf einer Pinnwand nicht mehr als Pull-Verfahren, sondern durch das Versenden der Änderungen mittels eines Gossip-Verfahrens, zu den Teilnehmern transportiert werden. Dadurch bleiben den Teilnehmern der regelmäßige Zugriff über die DHT zum Erhalten neuer Benachrichtigungen und somit eine Vielzahl an Zugriff und das Entschlüsseln der ABE verschlüsselten Daten erspart. Allerdings lässt der verwendete Gossip-Algorithmus Aufschlüsse über die Kontakte der Teilnehmer zu [50].

6.1.3 Blockieren von Nachrichten und Hash-Ketten

Die bis hierhin beschriebenen kryptographischen Verfahren tragen zur Zugriffskontrolle bei, können aber nicht verhindern, dass Nachrichten blockiert beziehungsweise nicht weitergeleitet werden. Bei einem sozialen Netzwerk mit einer Infrastruktur, die Server zur Kommunikation verwendet, kann einer der beteiligten Servern, die Nachricht unterschlagen, um die Verbreitung der Nachricht zu verhindern. Ebenso kann dieser Angriff in einem P2P-Netzwerk durch einen bösartigen Teilnehmer in der DHT oder einem Teilnehmer, der sich auf dem Übertragungsweg befindet, wie in einer Baumstruktur, durchgeführt werden. In den Verteilungsstrukturen von unstrukturierten Overlays, wie einem Gossip-Algorithmus, führt das Unterschlagen von Nachrichten nur bedingt zum Erfolg[35]. In einer baumartigen Verteilungsstruktur dagegen ist jeder Teilnehmer unterhalb des bösartigen Teilnehmers betroffen, wenn dieser keine Nachricht weiterleitet. Ist der bösartige Teilnehmer dabei in der

[34] Dies kann beispielsweise ein Server sein.

[35] Hierbei besteht die Möglichkeit, dass die Teilnehmer die Nachricht durch einen anderen Peer erhalten. Es ist also erforderlich, dass mehrere Teilnehmer die Nachricht nicht weiterleiten.

Lage, die Nachricht zu entschlüsseln, weil es sich beispielsweise um einen Pinnwandeintrag eines Teilnehmers handelt, den der bösartige Teilnehmer selber abonniert hat, so kann dieser auch gezielt Nachrichten unterschlagen. Um dies zu verhindern, können die Teilnehmer nach einiger Zeit den anderen Teilnehmer nach neuen Nachrichten anfragen oder zu jeder erhalten Nachricht eine Bestätigung zurückschicken, was allerdings zu einem höheren Nachrichtenaufkommen führt. Des Weiteren kann eine Bestätigung auch auf unbestimmte Zeit ausbleiben, wenn der Teilnehmer offline ist. In Megaphone [52] verwenden die Autoren eine fortlaufende Nummer, um fehlende Beiträge zu einer Pinnwand zu entdecken. Der Angreifer kann somit keine einzelnen Nachrichten unterschlagen, allerdings weiterhin alle Nachrichten blockieren. Dieser Angriff lässt sich durch Nachfragen eines Teilnehmers bei dem Besitzer der Pinnwand abwehren, wenn die Nachrichten eines Teilnehmers für längere Zeit ausbleiben. Der Teilnehmer, dem die Pinnwand gehört, kann bei diesem Verfahren nachträglich seine Pinnwandeinträge ändern, wenn ein Teilnehmer eine Änderungen nicht erhalten hat. Für dieses Problem können Hash-Ketten, wie in [54], eingesetzt werden. Hierbei wird ein Hashwert aus den Informationen einer Nachricht[36] mit einer Einweg-Hashfunktion erstellt und zusammen mit der Nachricht versendet. Bei der nächsten Nachricht wird der Hashwert aus den Informationen der neuen Nachricht und dem Hashwert der vorherigen Nachricht gebildet. Der Empfänger kann die Integrität der Nachricht überprüfen, indem er von der letzten überprüften Nachricht einer Pinnwand alle weiteren Hashwerte berechnet. Somit ergibt sich für alle weiteren Nachrichten eine Verkettung von Hashes, welche nur mit den vorherigen Nachrichten zu einem korrekten Ergebnis führen. Es können auch mehrere Hashes zu einer Nachricht hinzugefügt werden, solange für den Empfänger die Information vorliegt, welche Hashes in welcher Reihenfolge zusammenzuführen sind, um den Hashwert zur Überprüfung zu erzeugen. Wird der Hashwert, der letzten Nachricht, mit einer Signatur versehen, kann zusätzlich auch die Authentizität der Nachrichten geprüft werden. Das Erzeugen und anschließende Signieren eines Hashwertes einer Nachricht wird auch digitale Signatur genannt. Der Eigentümer der Pinnwand ist allerdings weiterhin in der Lage, seine Einträge auszutauschen, wenn der andere Teilnehmer über keinen aktuellen Beitrag verfügt. Somit ist es möglich, von dem letzten Stand, über den der Teilnehmer verfügt, eine neue Verkettung von Hashwerten mit Nachrichten aufzubauen. Hierbei muss der Angreifer allerdings wissen, was der letzte Stand ist, über den der Teilnehmer informiert wurde. Bei Fethr [54] wird hierfür vorgeschlagen, die Hashwerte von öffentlichen Pinnwandeinträge anderer Teilnehmer in

[36] Beispielsweise aus dem Nachrichtentext und den Metadaten, wie der Zeitpunkt, Ort, usw.

die eigenen mit einzuarbeiten. Der Nachteil durch die Verkettung ist, dass wenn ein Beitrag verloren geht, die gesamte Pinnwand möglicherweise nicht mehr überprüft werden kann und auch das Löschen oder Bearbeiten (beispielsweise Korrigieren von Fehlern) eines Eintrages durch den Teilnehmer nicht mehr möglich ist.

6.1.4 Diskussion

In diesem Abschnitt wurden verschiedene Kommunikationsmöglichkeiten und Zugriffskontrollen vorgestellt und welche Mechanismen dabei verwendet werden können. Die vorgestellten Verfahren verwenden bei der push-orientierten Kommunikation asymmetrische Verschlüsselungsverfahren zum Sicherstellen der Authentizität in Kombination mit symmetrischen Verfahren zum Schutz der Vertraulichkeit[37], da die lesenden Zugriffe hier im Vordergrund stehen. Um die Integrität bei diesem Nachrichtenfluss zu schützen, können auch Hashfunktionen beziehungsweise digitale Signaturen verwendet werden. Bei dieser Art der Verteilung kann es vorkommen, dass Informationen über die Kontakte eines Teilnehmers an andere Teilnehmer geraten. Ist die Privatsphäre für das soziale Netzwerk nicht ausschlaggebend, reicht an dieser Stelle auch die Verwendung digitaler Signaturen aus. Bei den Mechanismen, die die pull-orientierte Kommunikation umsetzen, wird auch mehr Flexibilität bei den schreibenden Zugriffen ermöglicht. Schreibende Zugriffe sind zwar auch bei den push-orientierten Verteilungsverfahren möglich, allerdings werden hierbei die bestehenden Nachrichten nicht verändert, sondern zusätzliche Nachrichten versendet, um eine Änderung abzubilden. Für anspruchsvolle und feingranulare Zugriffe werden Mechanismen, wie ABE und Zugriffskontrolllisten verwendet. Dabei lässt sich festhalten, dass die Verwendung des öffentlichen Schlüssels eines Teilnehmers, welcher mit der Identität des Teilnehmers verknüpft ist, um schreibende Zugriffe zu genehmigen, Informationsgewinnung für die Instanz, die die Daten beherbergt, ermöglicht. Der Einsatz von feingranularen Zugriffskontrollen kann in einer P2P-Umgebung zu Einschnitten bei der Performanz führen, weshalb versucht wird, diese Verfahren möglichst sparsam einzusetzen. In der Evaluation von [40] zeigt sich, dass die Engpässe nicht bei dem Hinzufügen neuer Daten entstehen, sondern in dem lesendem Zugriff, da viele Daten abgerufen und entschlüsselt werden müssen, um beispielsweise die Inhalte einer Profilseite darzustellen. Als Konsequenz daraus, kann das Überprüfen von Teilnehmerdaten erschwert sein, wenn dies regelmäßig geschieht. Auf diesen Aspekt wird im nächsten Abschnitt weiter eingegangen.

[37] Für eine praktische Umsetzung gilt es allerdings einige Fallstricke zu beachten [23].

Der Einsatz von asymmetrischer Kryptographie oder digitalen Signaturen bringt noch einen weiteren Aspekt, welcher in Abschnitt 3.3.4 unter Punkt eins schon angedeutet, aber noch nicht explizit angesprochen wurde. Dabei handelt es sich um die Umsetzung der Authentifizierung der Teilnehmer in sozialen Netzwerken ohne eine zentrale Organisationseinheit. Bei der Verwendung von einem Benutzernamen und Passwort, ohne eine zentrale vertrauenswürdige Instanz, müsste der Teilnehmer gegenüber jedem anderen Teilnehmer eine Kombination aus diesen beiden Merkmalen vergeben. Da dies unvorteilhaft ist, wird dies mittels der asymmetrischen Verschlüsselung umgesetzt. Dafür muss allerdings sichergestellt werden, dass die Teilnehmer zu ihren Kommunikationspartnern auch den korrekten zugehörigen öffentlichen Schlüssel besitzen. In sozialen Netzwerken kann hierfür der direkte Kontakt im realen Leben oder Empfehlungen von Freunden in dem Netzwerk zum Austausch dieser Schlüsseln genutzt werden [13]. Eine andere Möglichkeit ist das Beziehen des Schlüssels über die Einführung einer PKI, welche allerdings wieder die Problematik einer zentralen Instanz mit sich bringt (siehe hierzu Abschnitt 6.4.1). Um diese Nachteile zu vermeiden, gibt es auch Ansätze, PKIs zu dezentralisieren [46].

6.2 Nachweise

Die Verfahren zur Durchführung der Zugriffskontrolle zeigen, dass Daten wie Eigen- und Fremdaktionen sowie Verwaltungs- oder Profildaten vor unberechtigten Zugriffen geschützt werden können. Bei den Fremdaktionen muss allerdings sichergestellt werden, dass diese sich nicht reproduzieren lassen und einem Teilnehmer zugeordnet werden können. Dies unterscheidet sich von den anderen drei Kategorien, da beispielsweise ein Teilnehmer diese Daten bestimmen kann, ohne das ein anderer Teilnehmer beteiligt sein muss. Zu einer Fremdaktion gehören unter anderem Aktionen, die in der Verbindung mit einer Pinnwand stehen, wie *gefällt mir*-Angaben, Kommentare oder Retweets beziehungsweise eine Angabe darüber, wer den Beitrag geteilt hat. Ebenso können dies soziale Beziehungen, Gruppeneinladungen, Freundschaftsanfragen oder Profilbesuche sein. Damit diese Aktionen zugeordnet werden können, kommen erneut digitale Signaturen zum Einsatz. Dabei ist wichtig zu unterscheiden, dass sich die Information, ob zwei Teilnehmer eine soziale Beziehung haben, von dem Zugriffsrecht, dass ein Teilnehmer auf die Daten eines anderen Teilnehmers zugreifen kann, unterscheidet. Um die angesprochenen Punkte zu verdeutlichen, soll der folgende Anwendungsfall helfen. Alice ruft die Pinnwand von Bob auf und erhält hierdurch zwei Beiträge von Bob. Charlie hat einen der Beiträge kommentiert (siehe

Abbildung 14). Damit Alice überprüfen kann, dass der Beitrag wirklich von Bob stammt und nicht verändert wurde, muss ein Nachweis existieren. Dies wird über eine digitale Signatur erreicht, indem sie die Signatur mit dem öffentlichen Schlüssel von Bob überprüft und dazu die Hashwerte erzeugt. Gegebenenfalls müssen vorher Entschlüsselungen durchgeführt werden, da Daten durch die Zugriffskontrolle geschützt werden. Um den Kommentar von Charlie zu überprüfen, wird das gleiche Verfahren angewendet, allerdings muss hierbei auch sichergestellt werden, dass Charlies Kommentar zu dem Beitrag von Bob gehört. Dies kann erreicht werden, indem der Hashwert von Charlies Kommentar zusammen mit einer eindeutigen Referenz zu dem Kommentar von Bob gebildet wird. Andernfalls kann Bob diesen Kommentar für andere Beiträge oder ein anderer Teilnehmer, wie Alice, diesen für die eigene Pinnwand verwenden. Die Verknüpfung sollte zusätzlich so gewählt werden, dass es Bob nicht möglich ist, seinen Beitrag nachträglich zu verändern, ohne dass die Signatur von Charlie ungültig wird[38] (siehe Abbildung 15).

Schwieriger wird es, wenn Charlie seinen Kommentar entfernen möchte. Charlie kann dies zwar über die oben genannten Zugriffsmechanismen in Auftrag geben, aber solange ein Peer ein Datenobjekt mit der gültigen Signatur hält, kann das Objekt immer wieder eingespielt werden. Des Weiteren kann Bob oder einer der Datenhaltenden Peers behaupten, dass ein Auftrag zum Löschen des Objektes nie eingegangen ist. Das Löschen von Objekten wird auch in Cachet [50] erwähnt, aber die Umsetzung nur angedeutet. Eine Möglichkeit ist die Verwendung eines Proxys wie aus [39]. Damit kann das Löschen umgesetzt werden, indem kein Teilnehmer den Kommentar mehr entschlüsseln kann. Dafür ist es notwendig, dass selbst öffentliche Beiträge zu der digitalen Signatur zusätzlich verschlüsselt werden müssen. Eine andere Möglichkeit ist das Modell von Lockr, welches wie bereits oben schon angemerkt, ein Verfallsdatum enthält, wobei es sich um soziale Beziehungen und nicht um Pinnwandeinträge handelt. Dabei gehen die Autoren [60] davon aus, dass Nachweise über soziale Beziehungen gegenüber kommerziellen Diensten verwendet werden, welche digitale Signaturen verkaufen können, weshalb diese nicht an die andere Parteien übertragen werden dürfen. Der Nachweis über den Besitz einer sozialen Beziehung erfolgt mittels des *Witness Hiding Proof of Knowledge* (WHPOK) Protokolls aus [32], um eine bessere Performanz als bei einem *Zero-Knowledge* Protokoll zu erreichen. Dies ermöglicht es einem Teilnehmer, gegenüber einer anderen Instanz (Beispielsweise ein anderer Teilnehmer oder Anbieter) zu beweisen, dass der Teilnehmer für eine soziale Verbindung eine gültige Signatur besitzt, ohne diese Signatur übertra-

[38] Beispielweise die ID und die digitale Signatur von Bobs Kommentar.

gen zu müssen. Damit allerdings das Ablaufdatum überprüft werden kann, ohne die digitale Signatur direkt sehen zu müssen, wird ein Beziehungsschlüssel verwendet, welcher nach einer festgelegten Zeit ungültig wird. Um dies zu ermöglichen besteht der Beziehungsschlüssel aus einer Hash-Kette, mit der der Teilnehmer für jeden Tag einen neuen Hashwert berechnen kann. Die Berechnung des Hashwertes ist allerdings nur bis zum Verfallsdatum möglich. Bei dem Verfahren von Lockr, zeigt sich auch, dass die Information über eine soziale Beziehung von einem Zugriffsrecht unterscheidet. Die Information über eine soziale Beziehung kann beispielsweise in dem Profil eines Teilnehmers angezeigt werden und ist mittels eines Nachweises überprüfbar. Ein Nachweis dieser Art kann auch die Information über einen Profilbesuch sein. Auch hier muss wieder eine Eindeutigkeit gewährleistet werden, wie der konkrete Zeitpunkt und welches Profil von welchem Teilnehmer besucht wurde. Im Vergleich zu einem Nachweis über eine soziale Beziehung, ist diese Information meist nur für den Teilnehmer, der besucht wurde sichtbar. Es muss also kein Nachweis gegenüber anderen Teilnehmern stattfinden.

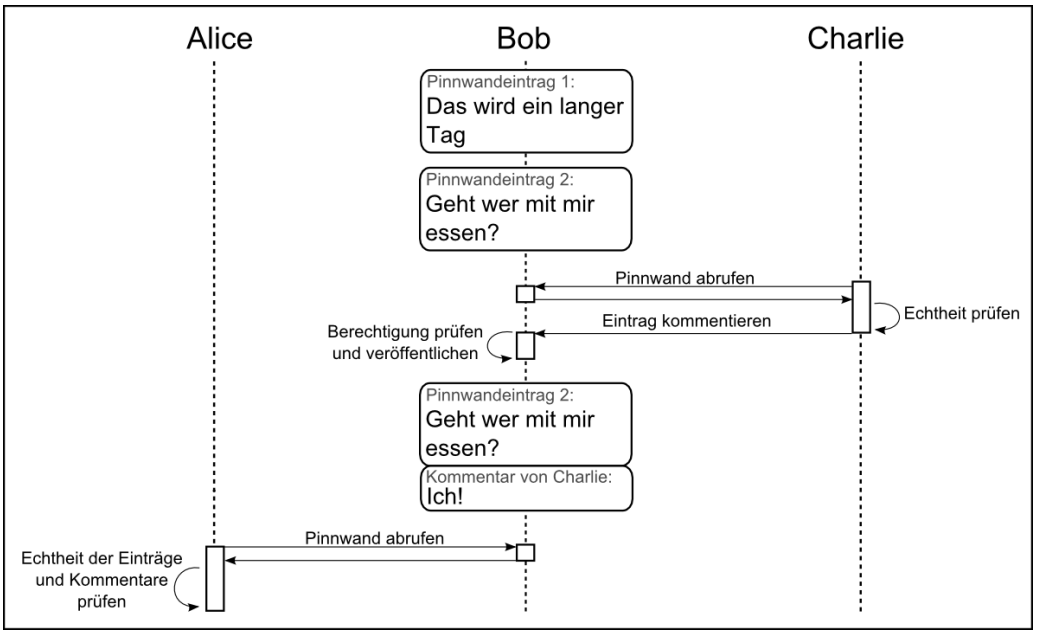

Abbildung 14: Fallbeispiel: Aufruf einer Pinnwand

6.2.1 Verdeckte Eigenaktionen

Als eine Herausforderung stellt sich die Erfassung von verdeckten Eigenaktionen in einer dezentrale Umgebung dar. Wie bereits in Abschnitt 4.3.2 beschrieben, handelt

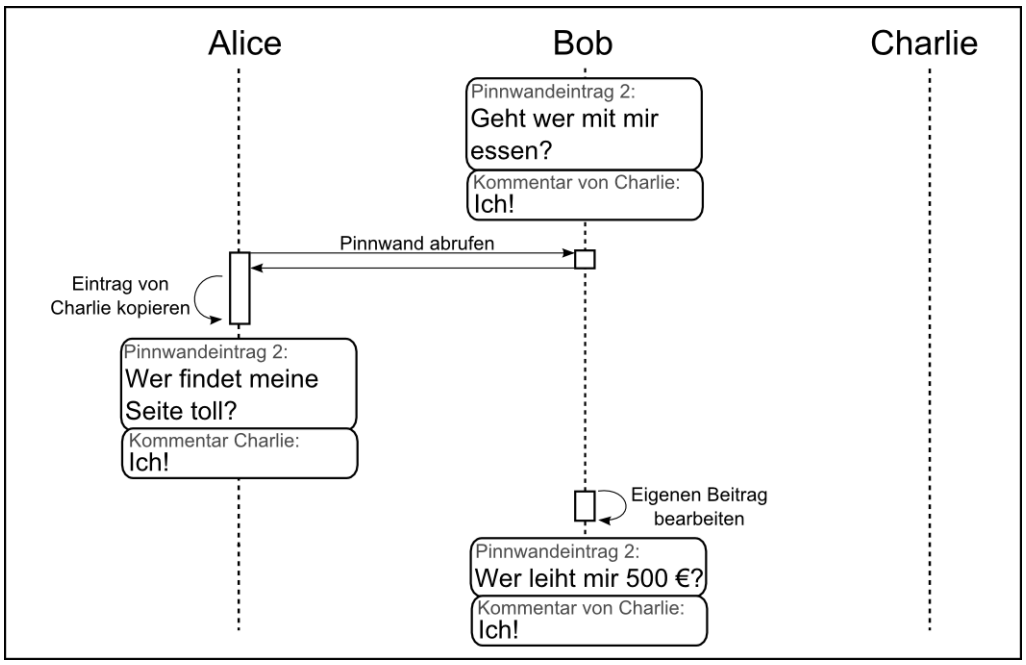

Abbildung 15: Fallbeispiel: Mögliche Manipulationen einer Pinnwand ohne direkte Zuordnung

es sich dabei beispielsweise um Suchanfragen oder Profilaufrufe. Suchanfragen lassen sich bei einer Infrastruktur mit dezentralen Servern von dem jeweiligen Server sammeln, wenn nicht mehrere Server verwendet werden. In einer P2P-Umgebgung hingegen, können jeweils andere Peers die Suchanfragen entgegen nehmen und beantworten, womit es erschwert ist, Daten über die Suchanfragen zu sammeln. Allerdings stellt sich hierbei auch die Frage, inwiefern die Suchanfragen authentisch vorliegen müssen, da andere Teilnehmer in der Regel auf diese Daten keinen Zugriff haben. Somit kann der Teilnehmer Daten zu seinen Suchanfragen (nur für sich selbst sichtbar) in seinem Profil hinterlegen, wenn er diese Informationen beispielsweise auf verschiedenen Endgeräten benötigt. Dabei sollten entsprechende kryptographische Verfahren verwendet werden, wenn die Speicherung auf nicht vertrauenswürdigen Instanzen getätigt wird. Ebenso verhält es sich bei den Profilaufrufen, wobei unterschieden werden kann, ob nur der Aufruf eines Profils gezählt oder die letzten Besucher angezeigt werden. Damit sich diese Daten nicht fälschen lassen, können hierbei die gleichen kryptographischen Verfahren, wie bei den Fremdaktionen verwendet werden. Dabei ist zu beachten, dass ein soziales Netzwerk einem Teilnehmer die Möglichkeit geben kann, die Aufrufe von Profilen vor anderen Teilnehmern zu

verbergen. Hierbei ist es notwendig, dass die Instanz, die die Profildaten eines Teilnehmers beherbergt, gegebenenfalls nicht erkennen kann, welcher Teilnehmer die Daten aufruft. Soll das soziale Netzwerk Profilaufrufe zählen, so gilt es, möglichst authentische Daten zu erzeugen, ohne dass der betroffene Teilnehmer erkennen kann, wer die Aufrufe durchgeführt hat. Eine Möglichkeit ist es, die Aufrufe von den Datenhaltenden Peers oder Servern zählen zu lassen. Sobald diese aber nicht vertrauenswürdig sind, erweist sich dies als schwierig, da diese Zählung manipuliert werden kann. Eine Möglichkeit hierzu bietet OverSoc [66], da hierbei die Daten eines Teilnehmers in einem DHT gehalten werden, der nur aus den sozialen Kontakten eines Teilnehmers besteht[39] und somit aus vertrauenswürdigen Peers. Dabei kann es allerdings zur Einschränkung der Verfügbarkeit der Daten des Teilnehmers kommen, wenn dieser nur über wenige Kontakte verfügt, weil er sich zum Beispiel neu in dem sozialen Netzwerk registriert hat. Des Weiteren kann es vorkommen, dass die Teilnehmer, zwischen denen eine soziale Beziehung besteht, oft in der gleichen Zeitzone leben und somit zu ähnlichen Zeiten on- oder offline sind [51].

6.2.2 Aggregierte und abgeleitete Daten eines Teilnehmers

Nachdem nun mögliche Mechanismen zum nachweisen einzelner Aktionsdaten vorgestellt wurden, werden in diesem Abschnitt Nachweise für Informationen, die sich auf mehrere Daten beziehen, behandelt. Die Aktionsdaten lassen sich über das Entschlüsseln und das Berechnen des Hashwertes der Signatur durch einen Teilnehmer nachweisen. Bei aggregierten Daten, wie die Anzahl der sozialen Kontakte eines Teilnehmers oder die durchschnittliche Anzahl an Teilungen pro Beitrag, gibt es dagegen keine Signatur, mit der die Echtheit dieser Werte bewiesen werden kann. Beispielsweise kann Alice hierfür alle ihre Freunde aufsummieren, die resultierende Information mit einer digitalen Signatur versehen und für andere Teilnehmer veröffentlichen. Um den Wert zu überprüfen, muss Bob trotzdem alle Nachweise über die sozialen Kontakte von Alice entschlüsseln und überprüfen, wenn er sichergehen will, dass Alices Angaben korrekt sind. Beziehen sich diese zusammengesetzten Informationen über eine komplette Historie von Alice, so kann dieser Schritt sehr aufwendig werden, wenn gleichzeitig rechenintensive kryptographische Verfahren zum Einsatz kommen (beispielsweise ABE). Ein weiteres Problem besteht dabei, wenn Bob nicht berechtigt ist, alle Daten von Alice einzusehen, da sie diese nur für eine andere Gruppe freigegeben hat oder zwischen den beiden keine soziale Beziehung besteht.

[39] Insofern der Teilnehmer ausreichend soziale Kontakte hat.

Trotzdem kann Alice aggregierte Informationen über sich für Bob freigeben, um ihre Glaubwürdigkeit zu erhöhen, beispielsweise indem sie anzeigt, dass sie genügend soziale Kontakte aufweisen kann, die ihr vertrauen. Da Bob aber nicht in der Lage ist, die einzelnen Signaturen abzurufen, da er nicht wissen soll, mit wem genau Alice befreundet ist, kann er sich auch nicht von der Echtheit der angegebenen Beziehungen überzeugen. Zu beachten ist hierbei, dass es sich nicht um das gleiche Problem handelt, welches zuvor mit dem WHPOK Protokoll gelöst wurde. Bei dem WHPOK Protokoll aus [32] wie es bei Lockr verwendet wird, beweist ein Teilnehmer, dass er über eine soziale Beziehung zu einer bestimmten Person verfügt, ohne den Datensatz mit der digitalen Signatur preisgeben zu müssen. Hierbei muss Alice allerdings beweisen, dass sie über eine Signatur verfügt, die nicht einer bestimmten Person zugeordnet werden darf, da Bob ansonsten weiß, welcher Teilnehmer mit Alice eine soziale Beziehung besitzt.

Eine mögliche Lösung, um den Missstand in diesen beiden Fällen zu beheben, ist die Überprüfung der Daten durch einen Prüfer. Bei dieser Überprüfung bekommt Teilnehmer (Charlie) Zugriff auf den zu prüfenden Teil der Daten von Alice und überprüft die Gültigkeit sowie die Echtheit der digitalen Signaturen. Danach erstellt Charlie eine digitale Signatur zu dem vorgegebenen Wert von Alice, um dessen Echtheit zu bestätigen. Dabei ergeben sich nun zwei weitere Probleme. Zum einen muss Alice gegenüber Charlie einige ihrer persönlichen Daten offenlegen und zum anderen sind die daraus entstandenen Werte nun von der Vertrauenswürdigkeit von Charlie abhängig. Diese Punkte müssen entsprechend bei dem Design der Mechanismen zur Überprüfung berücksichtig werden. Der erste Punkt betrifft die Auswahl eines oder mehrerer geeigneter Prüfer. Wird hierfür ein Peer aus der Liste der sozialen Kontakten von Alice gewählt, ergibt sich möglicherweise der Vorteil, dass dieser keine neuen Informationen erhält, da dieser Teilnehmer auch schon vorher die Kontakte von Alice kannte. Dies setzt voraus, dass es Teilnehmer gibt, die alle Kontakte oder andere aggregierte Daten sehen können. Dafür entsteht allerdings die Möglichkeit, dass Alice die Kontakte auswählt, die mit ihr kooperieren, um gefälschte Daten zu erzeugen. Die Alternative ist die Überprüfung durch zufällige Teilnehmer, wobei es erforderlich ist, dass Alice keine Möglichkeit hat Einfluss auf die Auswahl des Zeugens zu nehmen. In [35] verwenden die Autoren zur Auswahl eines zufälligen Peers Hashfunktionen, wobei ein Zeuge den Peers zugeordnet wird, die nahe zu seinem eigenen Hashwert sind. Bei dieser Überprüfung kommt es zwar zu der Verletzung der Privatsphäre von Alice, hat allerdings den Vorteil, dass ein unbekannter Teilnehmer möglicherweise kein Interesse an den Daten von Alice hat, im Vergleich zu einer ihr

bekannten Person [51].

Der zweite Punkt bezieht sich auf die Vertrauenswürdigkeit des Prüfers. Für Bob, der sich die Daten von Alice ansieht, ist wichtig für wie vertrauenswürdig er die Bewertung von Charlie einordnen kann. Wurde Charlie zufällig ausgewählt, so kann es für Bob von Relevanz sein, dass es mehrere Überprüfungen von unabhängigen Teilnehmern gab, um das Risiko eines Betrugs zu umgehen. Eine andere Möglichkeit kann das Bilden eines Vertrauenswertes sein, was sich auch bei der Auswahl von Prüfern durch Alice anwenden lässt. Hierbei berechnet Bob, inwiefern er einem Prüfer vertrauen kann, indem er beispielsweise ermittelt, ob zwischen ihm und einem der Prüfer eine soziale Beziehung und somit ein soziales Vertrauen besteht. Bestehen keine direkten Beziehungen, bieten sich verschiedene Strategien zum Sammeln von Informationen an, welche aus Vertrauens- oder Reputationsmodellen bekannt sind. Hierzu gehören unter anderem persönliche Erfahrungen, die ein Teilnehmer schon über vorherige Aktionen mit dem Prüfer sammeln konnte (lokale Informationen), eine transitive Kette von Vertrauen, bei der der Teilnehmer direkte soziale Kontakte nach der Vertrauenswürdigkeit des Zeugens befragt, welche wiederum ihre Kontakte befragen können oder auch eine globale Historie, in der alle Teilnehmer eintragen, welche Erfahrungen sie mit dem Prüfer beziehungsweise Teilnehmer gemacht haben [47].

Als letzten Punkt gilt es noch entsprechende Möglichkeiten einzurichten, um mit Fehlverhalten bei der Überprüfung umgehen zu können. Hierfür kann der geprüfte Teilnehmer und der Prüfer eine Bewertung abgeben, welche anschließend von den anderen Peers interpretiert werden. Durch ansteigende negative oder positive Bewertungen können die anderen Teilnehmer die Glaubwürdigkeit eines Prüfers oder geprüften Teilnehmers bewerten und ihre Bewertungen zu einer Überprüfung intepretieren. Möchte man allerdings einen Beweis haben, ob ein Teilnehmer sich korrekt verhalten hat, besteht die Möglichkeit die Abläufe festzuhalten, sodass für jeden Teilnehmer ein Beweis bei der Überprüfung entsteht. Um dies zu ermöglichen, führen Haeberlen et al. [35] in ihrem Verfahren Zeugen ein. Für jeden Teilnehmer werden mehrere Zeugen zufällig ausgewählt. Damit bei der Überprüfung kein Teilnehmer behaupten kann, dass ein Nachrichtenfluss stattfand beziehungsweise nicht stattfand, verwenden die Autoren jeweils ein Log pro Teilnehmer, der aus einer Hash-Kette besteht, damit nur neue Einträge angehangen werden können. Ein Eintrag bildet eine ein- oder ausgehende Aktion ab. Bei ausgehenden Aktionen wird der Eintrag der Hash-Kette signiert und an den anderen Teilnehmer gesendet. Somit entsteht mit diesem Eintrag ein dauerhafter Beleg für eine Aktion. Der Sender des Beleges erhält

ebenso eine Bestätigung des Empfängers. Um dieses Verfahren zu täuschen, kann einer der Teilnehmer ein zweites Log erstellen, damit es so aussieht, als hätte der andere Teilnehmer sich nicht korrekt verhalten. Damit dieses Problem gelöst wird, senden die Teilnehmer ihre Belege zu den jeweiligen Zeugen des anderen Teilnehmers. Die Belege kann der Zeuge später verwenden, um das Log ihres Teilnehmers auf Konsistenz zu prüfen. Des Weiteren lassen die Zeugen sich die neuen Logeinträge seit der letzten Überprüfung von ihrem Teilnehmer zukommen und überprüfen diese auf Fehler. Reagiert ein Teilnehmer nicht auf übermittelte Nachrichten, kann der andere Teilnehmer den Zeugen des Teilnehmers eine Nachricht zukommen lassen, sodass diese ein Challenge-Response-Verfahren durchführen, um zu prüfen, ob der Teilnehmer versucht, den anderen Teilnehmern zu täuschen oder dieser gegebenenfalls nicht mehr verfügbar ist.

6.2.3 Diskussion

Wie der vorherige Abschnitt zeigt, lassen sich als Nachweis von Aktionsdaten digitale Signaturen verwenden, wenn hierbei die entsprechenden Parameter für die Hashfunktion ausgewählt werden, damit eine eindeutige Zuordnung möglich ist. Problematisch erweist sich hierbei, dass diese Daten ungültig werden können, aber die Signatur weiterhin gültig ist. Um dies zu beheben, wird der Einsatz weiterer kryptographischer Verfahren oder Komponenten (beispielweise andere Peers als Proxy oder ein Auslaufdatum) benötigt. Ebenso stellt das Vorzeigen von digitalen Signaturen eine Schwierigkeit dar, wenn hierdurch die Vertraulichkeit der Informationen verletzt wird oder die Daten zusammengesetzt wurden. Ein vorgestellter Ansatz, ist die Überprüfung dieser Daten durch zufällige Teilnehmer, was zu einer nicht hinnehmbaren Verletzung der Privatsphäre führen kann. Hierbei gilt es also noch weitere Mechanismen einzubauen, die gegebenenfalls die Anonymität der Teilnehmer bei der Überprüfung gewährleisten. Als eine Alternative könnte dieses Verfahren nur bei neuen Teilnehmern oder Teilnehmern mit sehr wenigen sozialen Kontakten eingesetzt werden, da die Gefahr des *white washings*[40] besteht. Ein Teilnehmer meldet sich beispielsweise neu in dem Netzwerk an und erzeugt falsche Daten, um mit diesen andere Teilnehmer zu täuschen. Eine Überprüfung dieser Daten könnte dabei helfen, Angriffe dieser Art zu verhindern. Hierzu muss allerdings sichergestellt werden, dass erkannt werden kann, ob es sich um einen neuen Teilnehmer handelt. Die Verwen-

[40] Man spricht von white washing, wenn ein Teilnehmer sich nach dem Begehen von negativen Aktionen in dem Netzwerk erneut registriert und somit seine schlechten Bewertungen verloren gehen.

dung von Vertrauen bringt dabei den Vorteil, dass eine Verletzung der Privatsphäre umgangen werden kann, da ein vertraulicher Teilnehmer diese Daten schon kennt. Dies bietet allerdings den Raum für Absprachen unter befreundeten Teilnehmern, was durch eine zufällige Auswahl eines Teilnehmers erschwert wird. Beide Verfahren sind anfällig gegenüber Sybil-Angriffen, da ein Angreifer so die Chance erhöhen kann, eine Überprüfung seiner Daten durch eine seiner gesteuerten Identitäten vornehmen zu lassen. Ebenso gilt es noch zu evaluieren, inwiefern Rechenzeit durch diese Verfahren eingespart werden kann, im Vergleich zu einer Überprüfung von Daten, die beispielsweise mit ABE verschlüsselt sind. Des Weiteren müssen noch weitere Bereiche abgedeckt werden, unter anderem was mit einem Teilnehmer passiert, der seine Daten gefälscht hat oder diese nicht belegen möchte. Die Möglichkeiten können je nach Anwendungsfall variieren. In einem sozialen Netzwerk, in dem eine hohe Last durch Spam besteht, könnten beispielsweise die Teilnehmer erst das Lösen eines *Captchas* verlangen, bevor sie eine Nachricht akzeptieren. Alternativ könnte die Glaubwürdigkeit heruntergestuft oder der Peer von den anderen Teilnehmern isoliert werden. Die Verfahren für abgeleitete Daten können ebenso bei den aggregierten Daten für einen Teilnehmer angewendet werden. Dabei ist allerdings zu beachten, dass sich beide Teilnehmer über das Verfahren verständigen müssen, mit dem die neuen Informationen abgeleitet werden sollen. Hinsichtlich der verdeckten Eigenaktionen zeigt sich in diesem Abschnitt, dass eine stärkere Abhängigkeit im Vergleich zu den restlichen Aktionsdaten gegenüber der Infrastruktur des sozialen Netzwerkes besteht, wenn diese Daten erhoben werden sollen.

6.3 Aggregierte und abgeleitete Daten mehrerer Teilnehmer

Um die Daten von mehreren Teilnehmern zu aggregieren oder Informationen daraus abzuleiten, gilt es die Infrastruktur zu unterscheiden, in der die Daten gesammelt werden sollen. Handelt es sich um eine Infrastruktur mit dezentralen Servern, verfügen die Organisationseinheiten eventuell über die Daten von mehreren Teilnehmern und können diese direkt verarbeiten. Allerdings wird hierdurch nur ein Ausschnitt von Informationen ersichtlich, welcher möglicherweise nicht repräsentativ ist, um Informationen über einen größeren Bereich von Teilnehmern darzustellen, was dazu führt, dass die dezentralen Server gegebenenfalls untereinander Daten austauschen müssen. Zum anderen kann es vorkommen, dass die Organisationseinheiten durch den Einsatz von Verschlüsselung keinen Zugriff auf die Daten haben, womit sich eine ähnliche Situation wie in P2P-basierten sozialen Netzwerken ergibt. Hierbei

verfügt der Teilnehmer über seine Informationen und einige Informationen seiner sozialen Kontakte. Um nun aggregierte beziehungsweise abgeleitete Daten mehrerer Teilnehmer zu erheben, die über die bereits bekannten Informationen hinaus gehen, ist es erforderlich, dass die Teilnehmer ihre Informationen mit anderen Teilnehmern teilen. Problematisch bei beiden Situationen ist, dass die Daten, die herausgegeben werden, die Privatsphäre verletzen und die Performanz des Netzwerkes durch den dabei entstehenden Datenverkehr, beeinflussen können.

Betrachtet man die Verfahren aus Kapitel 4 zur Erkennung der Glaubwürdigkeit, werden hierbei vermehrt Informationen von Teilnehmern benötigt, die zu einem bestimmten Thema schreiben. Hierzu müssen also Beiträge zu einem Thema erfasst und von diesen Daten dann beispielsweise die Summe oder der Durchschnitt gebildet werden. Ein anderer Anwendungsfall kann das Anzeigen von kürzlich viel diskutierten Themen sein, was das Aufsummieren von aktuellen Beiträgen vieler Teilnehmer erfordert. Dagegen machen die vorgestellten Verfahren zur Erkennung von Spammern [7, 59] keinen Gebrauch von aggregierten oder abgeleiteten Daten mehrerer Teilnehmer. Es sollte also vorher bekannt sein, welche Daten benötigt werden, um eine Auswahl von konkreten Verfahren vornehmen zu können. Die Forschungsbereiche, die für eine Auswahl von Methoden in Betracht gezogen werden können, sind das Distributed Data Mining (DDM) und das Privacy-Preserving Distributed Data Mining (PPDDM). Die Verfahren im Bereich DDM, welche auch Lösungen für P2P-Netzwerke anbieten, ermöglichen einfache Operationen, wie die Berechnung der Summe eines Mehrheitsvotums oder des Durchschnitts. Basierend auf diesen einfachen Algorithmen können komplexe Verfahren aus dem Data Mining Bereich wie Assoziationsregeln oder K-Means Cluster [22] umgesetzt werden. Im Bereich PPDDM zielen die verschiedenen Verfahren darauf ab, Informationen mittels Data Mining zu beziehen, ohne die privaten Daten vor den jeweiligen Kommunikationspartnern enthüllen zu müssen, indem beispielsweise die Originaldaten mit einem Rauschen versehen werden. Problematisch dabei ist allerdings, dass die meisten Verfahren in diesem Bereich die Annahme treffen, dass die Teilnehmer sich semi-vertrauenswürdig verhalten. Das heißt, ein Teilnehmer folgt den Vorgaben des Protokolls und gibt seine Daten korrekt an. Er kann dabei allerdings versuchen, Informationen aus den Daten zu gewinnen, die er erhält [68]. Bhaduri et al. [9] dagegen gehen davon aus, dass ein Teilnehmer sich auch bösartig verhalten kann und beispielsweise das Protokoll nicht befolgt, sich mit anderen verschwört oder falsche Daten an gibt. Hierfür modellieren die Autoren PPDDM Algorithmen mittels Spieltheorie.

Um hier geeignete Verfahren auswählen und bewerten zu können, ist zum einen

die Festlegung auf eines der Verfahren und die dafür benötigten Informationen (beispielsweise ein Klassifizierer zur Bestimmung der Glaubwürdigkeit) notwendig. Zum anderen ist die Auswahl der verwendete Infrastruktur des sozialen Netzwerkes, wobei relevant ist, welche Instanzen Zugriff auf die Daten haben, erforderlich. Des Weiteren muss eine tiefere Auseinandersetzung mit den Verfahren aus den hier genannten Forschungsbereichen erfolgen. Dies würde allerdings den Rahmen für diese Arbeit überschreiten, weshalb die Betrachtung von Verfahren zur Sicherung von aggregierten und abgeleiteten Daten von mehreren Teilnehmern für weitere Arbeiten offen gelassen wird.

6.4 Verfahren zur Sybil-Abwehr

Ein Sybil-Angriff in sozialen Netzwerken kann zum einen dazu führen, dass Teilnehmerdaten erzeugt werden, womit ein Angreifer die Daten eines oder mehrerer Teilnehmer manipulieren kann. Beispielsweise kann diese eine aggregierte Information sein, wie die Anzahl der Freunde. Zum anderen können Sybils verwendet werden, um die Infrastruktur, wie etwa ein strukturiertes oder unstrukturiertes P2P-Overlay zu stören und damit beispielsweise das Blocken von Nachrichten ermöglichen. Des Weiteren können hierdurch Sicherheitsmechanismen ausgehebelt werden, wie beispielsweise die beschriebenen Verfahren zur Sicherstellung von aggregierten und abgeleiteten Daten. Aus diesen Gründen sollen an dieser Stelle auch Verfahren zur Abwehr von Sybil-Angriffen betrachtet werden.

Urdaneta et al. [61] unterscheiden sechs verschiedene Varianten von Verfahren zur Sybil-Abwehr. Dazu gehören zentralisierte Zertifizierung, verteilte Registrierung, physikalische Netzwerkeigenschaften, soziale Beziehungen zwischen den Teilnehmern, Spieltheorie und berechenbare Rätsel. Da Urdaneta et al. Verfahren aufbauend auf den sozialen Beziehungen und der zentralen Zertifizierung als am effektivsten zur Abwehr von Sybils beschreiben, werden diese Verfahren hier weiter vertieft und beschrieben, inwiefern sich diese Verfahren für soziale Netzwerke eignen.

6.4.1 Zentrale Zertifizierung

Bei den zentralen Zertifizierungsverfahren werden Zertifikate für die einzelnen Teilnehmer von einer vertrauenswürdigen Instanz vergeben. Das soziale Netzwerk kann dabei weiterhin eine dezentrale Infrastruktur besitzen, benötigt aber bei der Registrierung von neuen Teilnehmern die Unterstützung der zentralen Instanz. Das Zertifikat bindet einen öffentlichen Schlüssel an eine Identität, die der Teilnehmer in

dem Netzwerk verwenden kann. Dies wird bewerkstelligt, indem die zentrale Zertifizierungsstelle ein Root-Zertifikat ausstellt und das Zertifikat mit seinem privaten Schlüssel des dazugehörigen Root-Zertifikats signiert, so dass andere Teilnehmer nur den öffentlichen Schlüssel in dem Root-Zertifikat benötigen, um die Echtheit eines Zertifikates überprüfen zu können.[41] In dem Zertifikat sind unter anderem Daten, wie die Gültigkeitsdauer, der öffentliche Schlüssel und die Identität enthalten. Hiermit lassen sich auch statische Daten, wie das Registrierungsdatum oder die ID, sichern. Damit dabei die Anzahl der Sybils reduziert werden kann, muss die Zertifizierungsstelle eine Möglichkeit besitzen, eine reale Person von einem Sybil zu unterscheiden. Hierfür kommen Mechanismen außerhalb des Systems in der realen Welt zum Einsatz, wie die Kontrolle des Personalausweises. Als Alternative kann auch Geld bei jeder Registrierung verlangt werden [70]. Die Kritik an diesem Verfahren ist, dass zum einen die Hürde ein soziales Netzwerk zu nutzen durch die Kontrollen oder Kosten für aufrichtige Teilnehmer erhöht wird. Des Weiteren stellt eine zentrale Instanz einen Angriffspunkt für DoS-Angriffe sowie einen Flaschenhals bei der Performanz da, solange dieser Dienst nicht dezentralisiert wird [70]. Ebenso ergeben sich Nachteile aus dem Aufwand für die Administration einer zentralen Instanz und es muss ein Weg gefunden werden, dass alle dieser Instanz vertrauen.

Verfahren, die eine zentrale Authentifizierungsstelle verwenden, versuchen hierbei einige Nachteile auszugleichen. Die Infrastruktur von [20] verhindert beispielsweise, dass die Zertifizierungsstelle die Kommunikation der Teilnehmer durch das Wissen über die öffentlichen Schlüssel verfolgen kann. Das liegt daran, dass der Absender bei jedem Peer überschrieben wird (siehe Abschnitt 5.5.1). Außerdem merken die Autoren an, dass die die Zertifizierungsstelle auch dezentralisiert werden kann. Einen weiteren Vorteil nennen auch die Autoren aus [3], da die Zertifizierungsstelle hier nur einmal bei der Registrierung benötigt wird und danach nicht mehr.

6.4.2 Soziale Beziehungen

Die Verfahren zur Abwehr von Sybil-Angriffen in diesem Bereich können in *Sybil-Detektion* und *Sybil-Toleranz* unterteilt werden. Bei der Sybil-Detektion werden Sybil-Accounts erkannt und Maßnahmen von dem System eingeleitet. Im Vergleich dazu schränken Sybil-Toleranzverfahren den Einfluss, die ein Angreifer mit einem Sybilaccount ausüben kann, ein, statt Sybils direkt zu identifizieren. Dies wird, wie

[41] Nicht jedes Zertifikat muss durch das Zertifikat der Zertifizierungsstelle signiert sein, da sich hier Vertrauensketten bilden lassen. Eine Zertifizierungsstelle kann also ein Zertifikat ausstellen, mit dem wiederrum neue Zertifikate ausgestellt werden können [29].

in [62] beschrieben, dadurch erreicht, dass Aktionen in dem Netzwerk durch ein Guthaben limitiert werden. Das Guthaben bezieht sich auf die Verbindungen zwischen den Teilnehmern. Möchte ein Teilnehmer eine Aktion mit einem anderen Teilnehmer durchführen, muss auf dem Pfad zwischen den beiden Teilnehmern genug Guthaben für die Aktion zur Verfügung stehen. Dies bringt einige Vor- und Nachteile mit sich, allerdings ist ein wesentlicher Nachteil dabei, dass diese Verfahren nur für einige spezifische Anwendungsfälle funktionieren [62]. Aus diesem Grund wird der Fokus hier auf die Sybil-Detektionsverfahren gelegt. Sybil-Detektionsverfahren machen für eine korrekte Funktionsweise mehrere Annahmen, wobei die grundlegende Annahme ist, dass ein Angreifer viele Sybilaccounts erstellen kann, aber nur begrenzt soziale Verbindungen mit anderen Teilnehmern, sogenannten Angriffskanten, aufbauen kann [61]. Eine zweite wichtige Annahme ist, dass eine Region bestehend aus aufrichtigen Teilnehmern eine hohe Dichte von sozialen Beziehungen aufweist. Als dritte Annahme gilt, dass das System mindestens eine vertrauenswürdige Identität erhält [62]. Somit ergibt sich die Situation, dass das Netzwerk bestehend aus aufrichtigen Teilnehmern mit nur einigen wenigen Verbindungen zu dem Netzwerk bestehend aus Sybilaccounts verbunden ist (siehe Abbildung 16 a).

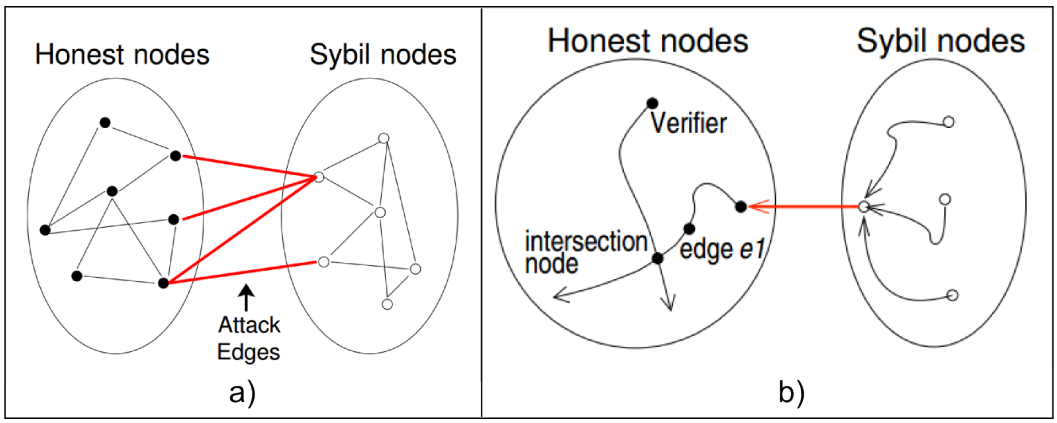

Abbildung 16: a) Angriffskanten zwischen einem Sybilnetzwerk und einem Netzwerk aus aufrichtigen Teilnehmern. b) Schnittpunkt bei einer Überprüfung. Beide entnommen aus [70]

Zwei Ausprägungen eines solchen Verfahrens, die auch in einer dezentralen Umgebung funktionieren, sind die Systeme SybilGuard [70] und SybilLimit [69], wobei SybilLimit eine Erweiterung von SybilGuard darstellt. Bei SybilGuard durchläuft jeder Teilnehmer das soziale Netzwerk beginnend von sich selbst mit einer bestimmten Länge mittels eines angepassten *Random Walks*. Jeder Teilnehmer verfügt über

einen öffentlichen und privaten Schlüssen sowie über eine IP-Adresse. Die öffentlichen Schlüssel der Teilnehmer, die durchlaufen werden, speichert der Teilnehmer in eine private Zeugentabelle zusammen mit der IP-Adresse. Gleichzeitig speichern alle Knoten, die durchlaufen werden für jede Kante von der ein Random Walk kommt, die öffentlichen Schlüssel in eine Registrierungstabelle. Möchte nun ein Teilnehmer (Prüfer) einen anderen überprüfen, schickt der zu überprüfende Teilnehmer seine Tabelle mit den öffentlichen Schlüsseln des Random Walks an den Prüfer. Der Prüfer vergleicht dann Überschneidungen mit dem eigenen Random Walk anhand der öffentlichen Schlüssel in den Tabellen. Da in der Zeugentabelle auch IP-Adressen angegeben sind, kann der Prüfer die Teilnehmer mit den Schnittpunkten anfragen, ob der Random Walk des zu prüfenden Teilnehmers diesen Teilnehmer wirklich durchlaufen hat (siehe Abbildung 16 b). Weitere Details dieses Verfahren können aus [70] entnommen werden.

Bei diesen Verfahren entstehen keine Hürden für die aufrichtigen Teilnehmer und die Nachteile einer zentralen Instanz können vermieden werden. Dafür benötigen sie die bereits aufgeführten Annahmen. Des Weiteren funktionieren sie am besten, wenn die aufrichtigen Teilnehmer dicht miteinander verknüpft sind, was in realen Situationen nicht zutreffen muss [62]. Bilden sich dabei mehrere Communities, können diese untereinander nicht mehr unterscheiden, welche dieser aus Sybilaccounts oder aufrichtigen Teilnehmern besteht (siehe Abbildung 17).

6.5 Diskussion

In den einzelnen Abschnitten wurde bereits diskutiert, wie sich die Mechanismen einsetzen lassen, um die Integrität und Authentizität von Teilnehmerdaten zu schützen und welche Auswirkungen dies auf die Privatsphäre haben kann. Da das Erfüllen von Schutzzielen an sich allerdings keinen Wert darstellt, sondern sich ihre Relevanz aus dem jeweiligen Szenario ergibt, soll an dieser Stelle betrachtet werden, in welchen Anwendungsfällen die vorgestellten Mechanismen geeignet sind. Verfahren zur Abwehr von Sybils werden an dieser Stelle nicht beschrieben, da sie wie bereits erwähnt, ein breiteres Anwendungsspektrum besitzen.

Der Einsatz der hier beschriebenen Mechanismen kann von verschiedenen Faktoren abhängen, wie für welchen Anwendungsfall das soziale Netzwerk konzipiert beziehungsweise verwendet wird[42], auf welche Infrastruktur das soziale Netzwerk aufbaut oder ob die Instanzen, die zum Verteilen von Nachrichten oder zum Speichern von

[42] Hierbei spielt auch die sozial-politische Situation aus Abschnitt 3.1 eine Rolle.

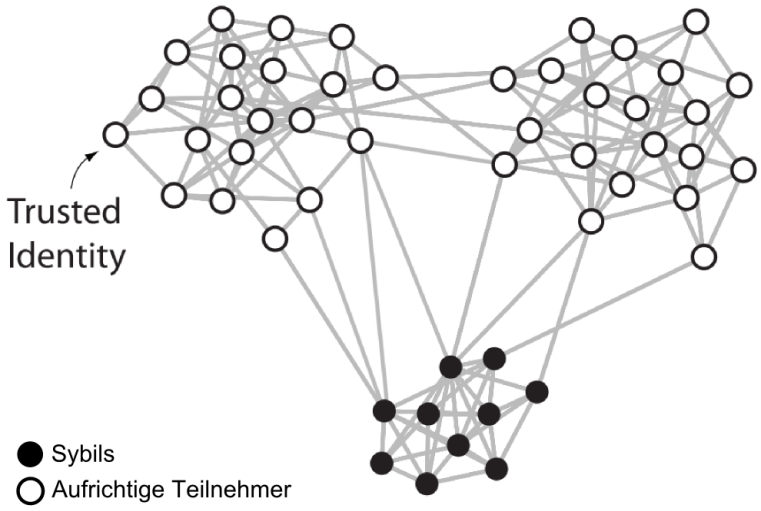

Abbildung 17: Die Sybil-Detektion mit mehreren Communities in einem sozialen Netzwerk, bei der die Unterscheidung zwischen Sybils und aufrichtigen Teilnehmern für den prüfenden Teilnehmer nicht mehr möglich ist. Modifiziert aus [62]

Daten verwendet werden, vertrauenswürdig sind. Eine öffentlich verfügbare Pinnwand braucht demnach keine Schutzmaßnahmen, um die Zugriffe vor den Datenhaltenden Instanzen zu verbergen. Bietet das soziale Netzwerk keine feingranularen Zugriffsrechte, da beispielsweise Beziehungen nur als Follower abgebildet werden, müssen auch keine aufwendigen Zugriffskontrollen eingesetzt werden. Allerdings bieten diese Verfahren oftmals einige Vorteile bei der Umsetzung beim Entziehen von Zugriffsrechten. Damit die Durchführung einer Aktion nachgewiesen werden kann, sollten Maßnahmen dagegen in jeder Situation Anwendung finden, bei der nicht vertrauenswürdige Instanzen beteiligt sind. Dabei können auch Verfahren helfen, die hier den Aufwand für die Überprüfung dieser Aktionen reduzieren, wenn es darum geht, die Daten auszuwerten, wie bei den abgeleiteten und aggregierten Daten eines Teilnehmers. Dabei stellt sich allerdings die Frage, wann ein Teilnehmer seine Daten fälscht. Ist dabei die reale mit virtuellen Identität verknüpft, ergibt sich möglicherweise der Vorteil, dass ein Teilnehmer bei einem Fehlverhalten in dem Netzwerk auch im realen Leben mit Konsequenzen rechnen muss und somit die Teilnehmer gehemmt sind aktiven Missbrauch zu betreiben. Wichtig dabei ist, dass es überhaupt eine Möglichkeit gibt, Missbrauch zu erkennen. In anderen Situationen, in denen auch verstärkt Austausch mit unbekannten Teilnehmern stattfindet, kann die

Hürde für den Missbrauch sinken. Ein typischer Anwendungsfall stellt die Twitter Suchfunktion da, bei der sich die aktuellen Beiträge zu einem Thema als Livestream verfolgen lassen. Alternativ dazu kann auch das Teilen von Beiträgen oder Retweeten in Betracht gezogen werden. Ein weiterer relevanter Punkt ist die Auswahl der Mechanismen nach den Informationen, die notwendig sind und die richtige Kombination von Mechanismen. Zum einen zeigt sich, dass nicht alle Verfahren auf abgeleitete und aggregierte Informationen mehrerer Teilnehmer angewiesen sind und zum anderen kann eine Methode zum Schutz der Vertraulichkeit von einem anderen Mechanismus ausgehebelt werden.

6.6 Zusammenfassung

In diesem Kapitel wurden Mechanismen zur Erfüllung der Schutzziele der Integrität und Authentizität für soziale Netzwerke, die über keine zentrale Organisationseinheit verfügen, vorgestellt. Hierfür wurden Mechanismen zur Umsetzung von Zugriffskontrollen für lesende und schreibende Zugriffe sowie für die Sicherstellung der Durchführung von Aktionen betrachtet. Bei der Sicherstellung der Durchführung von Aktionen von abgeleiteten und aggregierten Daten konnte nicht auf bestehende Verfahren von dezentralen sozialen Netzwerken zurückgegriffen werden, weshalb hier Verfahren aus den Bereichen *Accountability* in P2P-Netzwerken [35], Vertrauens- und Reputationsmanagement vorgestellt wurden. Dabei wurde aufgezeigt, wie sich diese Mechanismen einsetzen lassen, um Informationen zu überprüfen, auch wenn sie nicht von einem Teilnehmer direkt eingesehen werden können. Für diese Verfahren wurden ebenso die Auswirkungen auf die Privatsphäre diskutiert. Abschließend wurden Verfahren zur Bekämpfung von Sybilaccounts vorgestellt und die Anwendungsfälle der vorgestellten Mechanismen diskutiert.

7 Zusammenfassung, Fazit und Ausblick

Diese Arbeit hat sich der Zielstellung angenommen, geeignete Mechanismen zur Sicherung der Authentizität und Integrität in sozialen Netzwerken ohne eine zentrale Organisationseinheit zu identifizieren und zu bewerten. Hierfür wurden zuerst die Grundlagen im Bereich soziale Netzwerke, Schutzziele sowie Vertrauen, Reputation und Glaubwürdigkeit dargelegt. Danach wurden Bereiche für geeignete Mechanismen über die Analyse der Angriffe, Teilnehmerdaten und der verschiedenen Ausprägungen von dezentralen sozialen Netzwerken, ausgewählt. Innerhalb dieses dreiteiligen Prozesses wurden die Angriffe anhand des Modells von Paul et al. [51] analysiert und diskutiert. Dabei stellte sich heraus, dass die größte Gefahr von der Anwendungsebene ausgeht, weshalb der Fokus in den weiteren Kapiteln auf diese Ebene gelegt wurde. Die Analyse der Teilnehmerdaten wurde dazu verwendet, eine eigenen Kategorisierung aufzustellen, um die Eigenschaften der verschiedenen Daten hinsichtlich der Authentizität einordnen zu können. Der letzte Teil der Analyse bestand aus der Betrachtung der verschiedenen Dezentralisierungsformen und der Auswirkung auf die Teilnehmerdaten, wobei die eigene Kategorisierung verwendet wurde. Hierdurch konnten zum einen notwendige Mechanismen identifiziert werden und zum anderen wurde ersichtlich, welche Daten für welche Instanzen in der jeweiligen Form noch verfügbar sind. In dem letzten Kapitel wurden Mechanismen aus den Bereichen vorgestellt, welche im Laufe der Arbeit identifiziert werden konnten. Dabei wurde diskutiert, inwiefern dabei die Privatsphäre verletzt wird und wie diese Mechanismen die Authentizität und Integrität schützen.

7.1 Fazit

Hinsichtlich der Privatsphäre lässt sich festhalten, dass dezentrale Infrastrukturen in Kombination mit kryptographischen Verfahren in der Lage sind, wesentliche Funktionen eines sozialen Netzwerkes umzusetzen, ohne dabei die Identität der Teilnehmer preisgeben zu müssen. Gleichzeitig werden die Daten vor Zugriffen unberechtigter Personen geschützt, wobei dies nicht bedeutet, dass für Dritte kein Erkenntnisgewinn über die Teilnehmer mehr möglich ist. Wie ausgeprägt dieser Erkenntnisgewinn ist, hängt von der verwendeten Infrastruktur und den Mechanismen ab, wobei es zu differenzieren gilt, ob der Informationsgewinn auch eine relevante Verletzung der Privatsphäre darstellt. Dementsprechend gilt es für den jeweiligen Einsatzzweck des sozialen Netzwerkes eine geeignete Kombination von Infrastruktur und Sicherheitsmechanismen auszuwählen. Dabei zeigt sich auch, dass eine Infrastruktur, bestehend

aus einer zentralen Organisationseinheit mit P2P-Unterstützung, unpassend für den Schutz der Privatsphäre sein kann.

Um die Integrität und Authentizität von Teilnehmerdaten zu schützen, zeigen sich die Bereiche der Zugriffskontrolle, Sybil-Abwehr und Überprüfbarkeit von Daten als erachtenswert. Je nachdem wie elegant die Zugriffskontrolle und die Schlüsselrücknahme sein soll, benötigen diese Verfahren mehr bzw. weniger Rechenzeit. Dies führt direkt zum nächsten Punkt. Nämlich dem Einrichten von Nachweisen über durchgeführte Aktionen und Überprüfung dieser Nachweise mit einem angemessenen Aufwand. Dieser Aufwand kann durch Rechenzeit definiert sein oder davon abhängen, dass die Nachweise nicht einem anderen Teilnehmer vorgelegt werden müssen. Um dies zu adressieren, wurden Verfahren vorgestellt, welche eine direkte Kontrolle der Daten durchführen und somit eine Gefahr für die Verletzung der Privatsphäre, ähnlich wie bei der Verwendung einer zentralen Organisationseinheit, darstellen. Der wesentliche Unterschied dabei ist, dass ein Erkenntnisgewinn vermieden werden kann und somit auch keine Verletzung der Privatsphäre entsteht. Dabei existiert allerdings die Möglichkeit, den Mechanismus über kooperierende Gruppen zu umgehen. Alternativ dazu können mögliche Verletzungen der Privatsphäre in Kauf genommen werden, wofür es erschwert wird, die Kontrollsysteme auszuhebeln. Mittels der in dieser Arbeit behandelten Verfahren lassen sich Teilnehmerdaten sichern, sodass andere Verfahren, wie Glaubwürdigkeitsanalyse oder Spamerkenunngen auf diesen Daten aufbauen können, solange diese nicht abgeleitete beziehungsweise aggregierte Daten mehrerer Teilnehmer verwenden. Ebenso kann es zu Einschränkungen bei den verdeckten Eigenaktionen und durch die spezifischen Annahmen der jeweiligen Verfahren kommen. Des Weiteren gilt es zu berücksichtigen, dass die Sicherheit der Verfahren, die asymmetrische Kryptographie verwenden, von der Verteilung der Schlüssel abhängig sind.

Die eigene erstellte Kategorisierung von Teilnehmerdaten hat sich für die Analyse weitestgehend bewährt. Allerdings sind hierbei noch Modifikationen beziehungsweise Verbesserungen möglich, welche während der Diskussionen offensichtlich wurden. Zum einen lässt sich die Unterteilung von aggregierten und abgeleiteten Daten auch in aggregierte oder abgeleitete Daten eines bzw. mehrerer Teilnehmer ändern. Des Weiteren stellt sich bei P2P-basierten sozialen Netzwerken heraus, dass die notwendige Interaktion eines Teilnehmers auch ein Kriterium zur Unterscheidung bei den Fremdaktionen sein kann.

7.2 Ausblick

Da diese Arbeit selber keinen praktischen Anteil besitzt, bietet sich als nächster Schritt die Umsetzung und Evaluation der hier beschriebenen Verfahren an. Dazu gehören unter anderem die Mechanismen zur Überprüfung von aggregierten und abgeleiteten Daten von einem Teilnehmer, welche in dieser Form noch nicht in den hier behandelten sozialen Netzwerken verwendet wurden. Des Weiteren war es eine Motivation, dass Verfahren aus dem Data Mining verwendet werden können, um aufbauend auf den Daten eine Spamerkennung oder Glaubwürdigkeitsanalyse umzusetzen. Hierfür gilt es konkrete Verfahren zu entwickeln und hinsichtlich ihrer Performanz zu evaluieren sowie einen Vergleich zu bereits bestehenden Lösungen anzustreben. Da einige Verfahren abgeleitete und aggregierte Daten mehrerer Teilnehmer benötigen, ist an dieser Stelle eine weitere Bearbeitung der Thematik notwendig. Hierfür gilt es die Herausforderungen zu meistern, wie sich diese Daten austauschen lassen, ohne die Privatsphäre der Teilnehmer zu verletzten und gleichzeitig dafür zur sorgen, dass dabei die Anforderungen von authentischen und integeren Daten erfüllt wird. Dabei muss gegebenenfalls überprüft werden, ob es tragbare Kompromisse gibt, wenn sich diese Anforderungen nicht gemeinsam abbilden lassen. Eine Alternative zum Erheben der Daten über mehrere Teilnehmer, ist der Versuch die Data Mining-Verfahren mit den bestehenden Daten zu entwickeln. Hierbei gilt es zu evaluieren, welche Ergebnisse mit einer beschränkteren Datenauswahl erzielt werden können. Dabei ist zu beachten, dass diese Art der Daten über den für die grundlegende Funktionalität benötigten Anteil hinaus geht und somit möglicherweise Anreize notwendig sind, damit sich die Teilnehmer an einem solchen System beteiligen.

Obwohl in dieser Arbeit darauf Wert gelegt wurde, eine möglichst weitreichende Analyse von sozialen Netzwerken anzustreben, bietet diese Thematik noch Raum weitere für Analysen. Wie bei der Einteilung aus Abschnitt 5.1 angemerkt, gibt es noch einige Dezentralisierungsformen, von denen noch keine Ausprägungen entstanden sind. Hierbei könnten weitere Möglichkeiten zur Sicherung von Teilnehmerdaten entstehen, insofern sich diese Formen für die Anforderungen und Umsetzung von soziale Netzwerken als geeignet erweisen. Ebenso wurde der Fokus im Bereich der P2P-basierten sozialen Netzwerke auf strukturierte P2P-Overlays gelegt. Allerdings gibt es auch hier Ansätze, die unstrukturierte P2P-Overlays verwenden [1, 58], welche noch hinsichtlich der Zielstellung aus dieser Arbeit analysiert werden können.

Literatur

[1] S.M.A. Abbas, J.A. Pouwelse, D.H.J. Epema, and H.J. Sips. A gossip-based distributed social networking system. *2012 IEEE 21st International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 0:93–98, 2009. (Zitiert auf Seite 111)

[2] Alfarez Abdul-Rahman and Stephen Hailes. Supporting trust in virtual communities. In *Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 6 - Volume 6*, HICSS '00, pages 6007–, Washington, DC, USA, 2000. IEEE Computer Society. (Zitiert auf Seite 24)

[3] Luca Maria Aiello and Giancarlo Ruffo. Secure and flexible framework for decentralized social network services. In *PerCom Workshops*, pages 594–599, 2010. (Zitiert auf Seite 104)

[4] Dustin Bachrach, Christopher Nunu, Dan S. Wallach, and Matthew Wright. #h00t: Censorship resistant microblogging. *CoRR*, abs/1109.6874, 2011. (Zitiert auf Seite 63)

[5] Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, and Daniel Starin. Persona: an online social network with user-defined privacy. In *Proceedings of the ACM SIGCOMM 2009 conference on Data communication*, SIGCOMM '09, pages 135–146, New York, NY, USA, 2009. ACM. (Zitiert auf Seite 63, 87, 88, 89)

[6] Yahel Ben-David and Albert Kim. Robin: An attack-resilient microblogging service to circumvent government-imposed communication blackouts. (Zitiert auf Seite 10)

[7] Fabrício Benevenuto, Gabriel Magno, Tiago Rodrigues, and Virgílio Almeida. Detecting spammers on twitter. In *Proceedings of the 7th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS)*, 2010. (Zitiert auf Seite 10, 45, 102)

[8] Fabrício Benevenuto, Tiago Rodrigues, Meeyoung Cha, and Virgílio Almeida. Characterizing user behavior in online social networks. In *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, IMC '09, pages 49–62, New York, NY, USA, 2009. ACM. (Zitiert auf Seite 7, 41, 46, 52, 124)

[9] Kanishka Bhaduri, Kamalika Das, and Hillol Kargupta. Peer-to-peer data mining, privacy issues, and games. In *Autonomous Intelligent Systems: Multi-Agents and Data Mining*, pages 1–10. Springer, 2007. (Zitiert auf Seite 102)

[10] Joachim Biskup. *Security in Computing Systems: Challenges, Approaches and Solutions*. SpringerLink: Springer e-Books. Springer, 2009. (Zitiert auf Seite 20)

[11] Martin Böhringer and Alexander Richter. Adopting Social Software to the Intranet: A Case Study on Enterprise Microblogging. In Hartmut Wandke, editor, *Mensch und Computer 2009: Grenzenlos frei?*, München, 2009. Oldenbourg. (Zitiert auf Seite 19)

[12] Danah Boyd and Nicole B. Ellison. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1-2), November 2007. (Zitiert auf Seite 15)

[13] Sonja Buchegger, Doris Schiöberg, Le Hung Vu, and Anwitaman Datta. PeerSoN: P2P social networking - early experiences and insights. In *Proceedings of the Second ACM Workshop on Social Network Systems Social Network Systems 2009, co-located with Eurosys 2009*, pages 46–52, Nürnberg, Germany, March 31, 2009. (Zitiert auf Seite 6, 76, 77, 79, 93)

[14] John F. Buford, Heather Yu, and Eng Keong Lua. *P2P Networking and Applications*. Morgan Kaufmann series in networking. Elsevier Science, 2009. (Zitiert auf Seite 66, 81, 82)

[15] Carlos Castillo, Marcelo Mendoza, and Barbara Poblete. Information credibility on twitter. In *Proceedings of the 20th international conference on World wide web*, WWW '11, pages 675–684, New York, NY, USA, 2011. ACM. (Zitiert auf Seite 10, 24, 43)

[16] Ankit Singla Chi-Yao Hong, Giang Nguyen. P2p microblogging. 2010. (Zitiert auf Seite 76, 87)

[17] Jin-Hee Cho, Ananthram Swami, and Ing-Ray Chen. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 13(4):562–583, 2011. (Zitiert auf Seite 23)

[18] Dhuvra Chopra, Henning Schulzrinne, Enrico Marocco, and Emil Ivov. xn: security issues and solutions. *Communications Surveys Tutorials, IEEE*, 11(1):4–12, 2009. (Zitiert auf Seite 82)

[19] Leucio Antonio Cutillo, Mark Manulis, and Thorsten Strufe. Security and privacy in online social networks. In Borko Furht, editor, *Handbook of Social Network Technologies and Applications*, pages 497–522. Springer US, 2010. (Zitiert auf Seite 9, 15, 20, 21, 34, 47, 48)

[20] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE*, 47(12):94 –101, dec. 2009. (Zitiert auf Seite 6, 23, 27, 31, 76, 79, 81, 104)

[21] Anwitaman Datta, Sonja Buchegger, Le-Hung Vu, Thorsten Strufe, and Krzysztof Rzadca. Decentralized online social networks. In *Handbook of Social Network Technologies*, pages 349–378. 2010. (Zitiert auf Seite 6, 15, 16, 17, 75)

[22] S. Datta, K. Bhaduri, C. Giannella, R. Wolff, and H. Kargupta. Distributed data mining in peer-to-peer networks. *Internet Computing, IEEE*, 10(4):18–26, 2006. (Zitiert auf Seite 102)

[23] Don Davis. Defective sign & encrypt in s/mime, pkcs#7, moss, pem, pgp, and xml. In *USENIX Annual Technical Conference, General Track*, pages 65–78, 2001. (Zitiert auf Seite 92)

[24] Krishna Dhara, Yang Guo, Mario Kolberg, and Xiaotao Wu. Overview of structured peer-to-peer overlay algorithms. In Xuemin Shen, Heather Yu, John Buford, and Mursalin Akon, editors, *Handbook of Peer-to-Peer Networking*, pages 223–256. Springer US, 2010. (Zitiert auf Seite 76)

[25] Diaspora. Protocol overview. https://wiki.diasporafoundation.org/Federation_protocol_overview, 2013, Letzte Sichtung am 12.10.2013. (Zitiert auf Seite 70)

[26] Diaspora. Architecture overview. https://wiki.diasporafoundation.org/Architecture_overview, 2013, Letzte Sichtung am 13.10.2013. (Zitiert auf Seite 6, 72)

[27] John R. Douceur. The sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, pages 251–260, London, UK, UK, 2002. Springer-Verlag. (Zitiert auf Seite 33)

[28] Claudia Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg Wissensch.Vlg, 2009. (Zitiert auf Seite 20)

[29] Bundesamt für Sicherheit in der Informationstechnik. Sicherheitsmechanismen in elektronischen ausweisdokumenten. https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Sicherheitsmechanismen/sicherPKI/pki_node.html, o.J., Letzte Sichtung am 23.11.2013. (Zitiert auf Seite 104)

[30] J. Golbeck. Computing with trust: Definition, properties, and algorithms. In *Securecomm and Workshops, 2006*, pages 1–7, 2006. (Zitiert auf Seite 23)

[31] Jennifer Golbeck. The dynamics of web-based social networks: Membership, relationships, and change. *First Monday*, 12(11), 2007. (Zitiert auf Seite 16)

[32] Shafi Goldwasser and Erez Waisbard. Transformation of digital signature schemes into designated confirmer signature schemes. In Moni Naor, editor, *Theory of Cryptography*, volume 2951 of *Lecture Notes in Computer Science*, pages 77–100. Springer Berlin Heidelberg, 2004. (Zitiert auf Seite 94, 98)

[33] T. Grandison and M. Sloman. A survey of trust in internet applications. *Communications Surveys Tutorials, IEEE*, 3(4):2–16, 2000. (Zitiert auf Seite 23)

[34] Manish Gupta, Peixiang Zhao, and Jiawei Han. Evaluating event credibility on twitter. In *SDM*, pages 153–164, 2012. (Zitiert auf Seite 10, 24, 43)

[35] Andreas Haeberlen, Petr Kouznetsov, and Peter Druschel. Peerreview: practical accountability for distributed systems. *SIGOPS Oper. Syst. Rev.*, 41(6):175–188, October 2007. (Zitiert auf Seite 98, 99, 108)

[36] Brian Hilligoss and Soo Young Rieh. Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. *Inf. Process. Manage.*, 44(4):1467–1484, July 2008. (Zitiert auf Seite 24)

[37] Facebook Inc. Informationen, die wir über dich erhalten. https://www.facebook.com/about/privacy/your-info, 2013, Letzte Sichtung am 6.10.2013. (Zitiert auf Seite 42, 54)

[38] Ed. J Pouwelse. Media without censorship (censorfree) scenarios draft-pouwelse-censorfree-scenarios-02. http://tools.ietf.org/html/draft-pouwelse-censorfree-scenarios-02, October 2012, Letzte Sichtung am 20.08.2013. (Zitiert auf Seite 10)

[39] Sonia Jahid, Prateek Mittal, and Nikita Borisov. Easier: encryption-based access control in social networks with efficient revocation. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 411–415, New York, NY, USA, 2011. ACM. (Zitiert auf Seite 89, 94)

[40] Sonia Jahid, Shirin Nilizadeh, Prateek Mittal, Nikita Borisov, and Apu Kapadia, Kapadia. Decent: A decentralized architecture for enforcing privacy in online social networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pages 326–332, 2012. (Zitiert auf Seite 76, 89, 90, 92)

[41] Xing Jin and S.-H.Gary Chan. Unstructured peer-to-peer network architectures. In Xuemin Shen, Heather Yu, John Buford, and Mursalin Akon, editors, *Handbook of Peer-to-Peer Networking*, pages 117–142. Springer US, 2010. (Zitiert auf Seite 75)

[42] Pierre St. Juste, Heungsik Eom, Kyungyong Lee, and Renato J. O. Figueiredo. Enabling decentralized microblogging through p2pvpns. In *CCNC*, pages 323–328, 2013. (Zitiert auf Seite 77)

[43] Byungkyu Kang, John O'Donovan, and Tobias Höllerer. Modeling topic specific credibility on twitter. In *Proceedings of the 2012 ACM international conference on Intelligent User Interfaces*, pages 179–188. ACM, 2012. (Zitiert auf Seite 10, 44)

[44] Michal Kryczka, Ruben Cuevas, Carmen Guerrero, Eiko Yoneki, and Arturo Azcorra. A first step towards user assisted online social networks. In *Proceedings of the 3rd Workshop on Social Network Systems*, SNS '10, pages 6:1–6:6, New York, NY, USA, 2010. ACM. (Zitiert auf Seite 6, 66, 68)

[45] Merriam-Webster Lexikon. Credibility. http://www.merriam-webster.com/dictionary/credibility, o.J., Letzte Sichtung am 28.01.2013. (Zitiert auf Seite 24)

[46] Zhongwen Li, Xiaochen Xu, Liang Shi, Jian Liu, and Chen Liang. Authentication in peer-to-peer network: Survey and research directions. In *Network and System Security, 2009. NSS '09. Third International Conference on*, pages 115–122, 2009. (Zitiert auf Seite 93)

[47] Sergio Marti and Hector Garcia-Molina. Taxonomy of trust: categorizing p2p reputation systems. *Comput. Netw.*, 50(4):472–484, March 2006. (Zitiert auf Seite 99)

[48] Giuliano Mega, Alberto Montresor, and Gian Pietro Picco. Efficient dissemination in decentralized social networks. In *Peer-to-Peer Computing (P2P), 2011 IEEE International Conference on*, pages 338–347, 2011. (Zitiert auf Seite 77)

[49] Meredith Ringel Morris, Scott Counts, Asta Roseway, Aaron Hoff, and Julia Schwarz. Tweeting is believing?: understanding microblog credibility perceptions. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, CSCW '12, pages 441–450, New York, NY, USA, 2012. ACM. (Zitiert auf Seite 10)

[50] Shirin Nilizadeh, Sonia Jahid, Prateek Mittal, Nikita Borisov, and Apu Kapadia. Cachet: a decentralized architecture for privacy preserving social networking with caching. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, CoNEXT '12, pages 337–348, New York, NY, USA, 2012. ACM. (Zitiert auf Seite 76, 90, 94)

[51] Thomas Paul, Benjamin Greschbach, Sonja Buchegger, and Thorsten Strufe. Exploring decentralization dimensions of social networking services: adversaries and availability. In *Proceedings of the First ACM International Workshop on Hot Topics on Interdisciplinary Social Networks Research*, HotSocial '12, pages 49–56, New York, NY, USA, 2012. ACM. (Zitiert auf Seite 6, 7, 28, 31, 33, 61, 62, 97, 99, 109)

[52] T. Perfitt and B. Englert. Megaphone: Fault tolerant, scalable, and trustworthy p2p microblogging. In *Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on*, pages 469–477, 2010. (Zitiert auf Seite 6, 76, 77, 80, 87, 91)

[53] Peter Saint-Andre, Kevin Smith, and Remko Tronçon. *XMPP: The Definitive Guide: Building Real-Time Applications with Jabber Technologies*. O'Reilly Media, Inc., 1 edition, April 2009. (Zitiert auf Seite 70)

[54] Daniel R. Sandler and Dan S. Wallach. Birds of a fethr: open, decentralized micropublishing. In *Proceedings of the 8th international conference on Peer-to-peer systems*, IPTPS'09, pages 1–1, Berkeley, CA, USA, 2009. USENIX Association. (Zitiert auf Seite 69, 91)

[55] Fabian Schneider, Anja Feldmann, Balachander Krishnamurthy, and Walter Willinger. Understanding online social network usage from a network perspective. In *Internet Measurement Conference*, pages 35–48, 2009. (Zitiert auf Seite 41, 47)

[56] Bruce Schneier. A taxonomy of social networking data. *Security and Privacy*, 8, 2010. (Zitiert auf Seite 47)

[57] Amre Shakimov, Harold Lim, Ramón Caceres, Landon P. Cox, Kevin Li, Dongtao Liu, and Alexander Varshavsky. Vis-à-vis: Privacy-preserving online social networking via virtual individual servers. In *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on*, pages 1–10, 2011. (Zitiert auf Seite 71)

[58] Rajesh Sharma and Anwitaman Datta. Supernova: Super-peers based architecture for decentralized online social networks. In *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on*, pages 1–10. IEEE, 2012. (Zitiert auf Seite 111)

[59] Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Detecting spammers on social networks. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 1–9, New York, NY, USA, 2010. ACM. (Zitiert auf Seite 10, 45, 102)

[60] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali, and Alec Wolman. Lockr: better privacy for social networks. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, CoNEXT '09, pages 169–180, New York, NY, USA, 2009. ACM. (Zitiert auf Seite 87, 94)

[61] Guido Urdaneta, Guillaume Pierre, and Maarten Van Steen. A survey of dht security techniques. *ACM Comput. Surv.*, 43(2):8:1–8:49, February 2011. (Zitiert auf Seite 82, 103, 105)

[62] Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel, Krishna P Gummadi, Alan Mislove, and Ansley Post. Exploring the design space of social network-based sybil defenses. In *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on*, pages 1–8. IEEE, 2012. (Zitiert auf Seite 6, 105, 106, 107)

[63] Stanley Wasserman and Katherine Faust. *Social network analysis: Methods and applications*, volume 8. Cambridge university press, 1994. (Zitiert auf Seite 15)

[64] David Westerman, Patric R. Spence, and Brandon Van Der Heide. A social network as information: The effect of system generated reports of connectedness on credibility on twitter. *Computers in Human Behavior*, 28(1):199 – 206, 2012. (Zitiert auf Seite 10)

[65] Alan F. Westin. *Privacy and Freedom*. Springer, New York, 1967. (Zitiert auf Seite 22)

[66] D.I. Wolinsky, P.S. Juste, P.O. Boykin, and R. Figueiredo. Oversoc: Social profile based overlays. In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on*, pages 205–210, 2010. (Zitiert auf Seite 23, 76, 97)

[67] Tianyin Xu, Yang Chen, Jin Zhao, and Xiaoming Fu. Cuckoo: towards decentralized, socio-aware online microblogging services and data measurements. In *Proceedings of the 2nd ACM International Workshop on Hot Topics in Planet-scale Measurement*, HotPlanet '10, pages 4:1–4:6, New York, NY, USA, 2010. ACM. (Zitiert auf Seite 6, 66, 68)

[68] Zhuojia Xu and Xun Yi. Classification of privacy-preserving distributed data mining protocols. In *Digital Information Management (ICDIM), 2011 Sixth International Conference on*, pages 337–342, 2011. (Zitiert auf Seite 102)

[69] Haifeng Yu, P.B. Gibbons, M. Kaminsky, and Feng Xiao. Sybillimit: A near-optimal social network defense against sybil attacks. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 3–17, 2008. (Zitiert auf Seite 105)

[70] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham Flaxman. Sybilguard: Defending against sybil attacks via social networks. *SIGCOMM Comput. Commun. Rev.*, 36(4):267–278, August 2006. (Zitiert auf Seite 6, 104, 105, 106)

[71] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. Privacy and security for online social networks: challenges and opportunities. *Network, IEEE*, 24(4):13–18, 2010. (Zitiert auf Seite 22)

[72] CSG ETH Zurich. Twimight für twitter. https://play.google.com/store/apps/details?id=ch.ethz.twimight, August 2013, Letzte Sichtung am 06.10.2013. (Zitiert auf Seite 10)

Anhang

Anhang

A Kategorisierungen von Teilnehmerdaten

Accountdaten	
Profildaten	Pseudonym Beschreibung Profilbild E-Mailadresse Wohnort
Verwaltungsdaten	Kreditkartennummer Alter vollständiger Name Anschrift
Statische Daten	Registrierungsdatum ID

Tabelle 2: Beispielmerkmale für Accountdaten der eigenen Kategorisierung

Aktionsdaten	
Eigenaktionen (verdeckt)	Profil aufrufen Fotoalben anschauen Suchen
Eigenaktion (sichtbar)	Beitrag schreiben Fotos hochladen Profil bearbeiten
Fremdaktionen (verdeckt)	Profil aufrufen
Fremdaktion (sichtbar)	Freundschaftsanfrage stellen Beitrag kommentieren Profil aufrufen Einen anderen Beitrag teilen oder *retweeten*
Metadaten	Absender einer Nachricht Empfänger einer Nachricht Zeitpunkt einer Aktion IP-Adresse des Nutzers
Inhalte	Bild Text Link Datum der Erstellung des Bildes

Tabelle 3: Beispielmerkmale für Aktionsdaten der eigenen Kategorisierung

Aggregierte Daten	
Eines Teilnehmers	Anzahl an Beiträgen Durchschnittliche Retweets pro Beitrag Anzahl an Kommentaren pro Beitrag Beiträge pro Tag
Mehrerer Teilnehmer	Anzahl an Tweets pro Minute Durchschnittliche Anzahl an Tweets pro Teilnehmer Teilnehmer mit den meisten Kommentaren Beitrag mit den meisten Retweets

Abgeleitete Daten	
Eines Teilnehmers	Tweet zu einem Thema Teilnehmer hat am meisten Beiträge zu Thema XY Freundschaftsbeziehung mit XY
Mehrerer Teilnehmer	Aktuelle Themen Alle Teilnehmer die zu einem Thema kommunizieren Häufigste verwendete URL zu einem Thema

Tabelle 4: Beispielmerkmale für aggregierte und abgeleitete Daten der eigenen Kategorisierung

Category	Description of activity
Search	Universal search
Scrapbook	Browse scraps Write scraps
Testimonials	Browse testimonials received Write testimonials Browse testimonials written
Videos	Browse the list of favorite Browse a favorite video
Photos	Browse a list of album Browse photo albums Browse photos Browse photos user was tagged Browse photo comments Edit and organize photos
Profile and Friends	Browse profiles Browse Homepage Browse list of friends Manage friend invitations Browse friends update Browse member communities Profile editing Browse fans Browse user lists Manage user events
Communities	Browse a community Browse a topic in a community Join or leave communities Browse members in communities Browse the list of community topics Post in a community topic Community management Accessing polls in communities Browse the list of communities Manage community invitations Community events
Other	Accessing applications User settings Spam folder, feeds, captcha Account login and deletion

Tabelle 5: Kategorisierung von Aktivitäten aus dem sozialen Netzwerk Orkut entnommen aus [8]

B Überblick der Teilnehmerdaten in den Dezentralisierungsformen

Zentrale Organisationseinheit

Accoundaten	
Profildaten	Durch die z.O. gesammelt
Verwaltungsdaten	Durch die z.O. gesammelt und überprüft
Statische Daten	Durch die z.Og. festgelegt

Aktionsdaten	
Eigenaktion	Werden von der z.O. gesammelt
Fremdaktion	Durch Vertrauen in die z.O. gesichert
Inhalte	Komplett für die z.O. sichtbar mit Ausnahmen bei Kryptographie
Metadaten	Komplett für die z.O. sichtbar mit Ausnahmen bei Kryptographie

Aggregierte und abgeleitete Daten			
Ein Teilnehmer	Durch die z.O. gesammelt	**Mehrere Teilnehmer**	Durch die z.O. gesammelt

Tabelle 6: Überblick zu den Teilnehmerdaten bei zentralen Organisationseinheiten (Abkürzungen: z.O. = zentrale Organisationseinheit, O. = Organisationseinheit)

Zentrale Organisationseinheit mit P2P Unterstützung

Accoundaten	
Profildaten	Durch die z.O. gesammelt
Verwal-tungsdaten	Durch die z.O. gesammelt und überprüft
Statische Daten	Durch die z.Og. fesgelegt

Aktionsdaten	
Eigenaktion	Im P2P-Netzwerk, ggf. Kopie an die z.O.
Fremdaktion	Im P2P-Netzwerk, ggf. Kopie an die z.O.
Inhalte	Wird ggf. an die z.O. übertragen oder abgerufen
Metadaten	Werden ggf. an die z.O. zusätzlich übertragen

Aggregierte und abgeleitete Daten			
Ein Teilnehmer	Gesammelt durch die z.O. oder Statistiken an die z.O. und jeder Peer sammelt für sich	**Mehrere Teilnehmer**	Statistiken an die z.O.

Tabelle 7: Überblick zu den Teilnehmerdaten bei zentralen Organisationseinheiten mit P2P-Unterstützung (Abkürzungen: z.O. = zentrale Organisationseinheit, O. = Organisationseinheit)

Dezentrale Server

Accoundaten	
Profildaten	Werden von der jeweiligen O. gesammelt
Verwaltungsdaten	Werden von der jeweiligen O. gesammelt und nach eigenem Ermessen geprüft
Statische Daten	Durch die jeweilige O. festgelegt

Aktionsdaten	
Eigenaktion	Durch Vertrauen in die O. oder Nachweise
Fremdaktion	Durch Vertrauen in die O. oder Nachweise
Inhalte	Verschlüsselt oder für die Server einsehbar
Metadaten	Für die beteiligten Server sichtbar

Aggregierte und abgeleitete Daten			
Ein Teilnehmer	Für eine Teilmenge gesammelt von den O.	**Mehrere Teilnehmer**	Für eine Teilmenge gesammelt von den O.

Tabelle 8: Überblick zu den Teilnehmerdaten bei dezentralen Server (Abkürzungen: z.O. = zentrale Organisationseinheit, O. = Organisationseinheit)

Soziales Netzwerk auf P2P-Basis

Accoundaten	
Profildaten	Vom jeweiligen Peer eingetragen
Verwaltungsdaten	Überprüfung durch jeden Peer selbst oder zusätzliche z.O.
Statische Daten	Noch keine Lösung besprochen.

Aktionsdaten	
Eigenaktion	Werden vom Peer selbst oder gar nicht gesammelt
Fremdaktion	Nachweise erforderlich. Soziales Vertrauen?
Inhalte	I.d.R. verschlüsselt
Metadaten	Vom Verfahren abhängig

Aggregierte und abgeleitete Daten			
Ein Teilnehmer	Sammelt der Peer selbst. Benötigt ggf. Informationen von anderen Peers	**Mehrere Teilnehmer**	Nur Informationen über soziale Beziehungen

Tabelle 9: Überblick zu den Teilnehmerdaten bei P2P-basierte sozialen Netzwerken (Abkürzungen: z.O. = zentrale Organisationseinheit, O. = Organisationseinheit)

Eidesstattliche Erklärung

Ich versichere, die von mir vorgelegte Arbeit selbständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Gummersbach, den 2. Dezember 2013

Benjamin Krumnow